

2022-1361

---

United States Court of Appeals  
for the  
Federal Circuit

---

LONGHORN HD LLC.,

*Appellant*

v.

UNIFIED PATENTS, LLC,

*Appellee*

---

Appeal from the Patent and Trademark Appeal Board

Case No. IPR2020-00879

Karl D. Easthom, Garth D. Baer, and Matthew S. Meyers  
Administrative Patent Judges

---

**APPELLANT'S PRINCIPAL AND OPENING BRIEF**

---

Alfred R. Fabricant  
Peter Lambrianakos  
Vincent J. Rubino, III  
Enrique W. Iturralde

*Attorneys for Appellant*

June 22, 2022

FABRICANT LLP  
411 Theodore Fremd Avenue  
Suite 206 South  
Rye, New York 10580  
(212) 257-5797  
ffabricant@fabricantllp.com  
plambrianakos@fabricantllp.com  
vrubino@fabricantllp.com  
eiturralde@fabricantllp.com

---

**PATENT CLAIMS AT ISSUE**

**U.S. PATENT NO. 7, 260,846 (Appx055)**

7. An intrusion detection method comprising the steps of: monitoring network traffic passing across a network communications path; extracting network packets from said passing traffic; storing individual components of said network packets in a database; constructing multi-dimensional vectors from at least two of said stored individual components and applying at least one multi-variate analysis to said constructed multi-dimensional vectors, said at least one multi-variate analysis producing a corresponding output set; establishing a correlation between individual output sets based upon a selected metric to identify anomalous behavior; and, classifying said anomalous behavior as an event selected from the group consisting of a network fault, a change in network performance and a network attack.

8. The method of claim 7, wherein said storing step comprises the steps of: identifying protocol boundaries in each extracted network packet; and, storing data from each field separated by said identified protocol boundaries in a separate record in said database.

10. The method of claim 7, wherein said step of applying at least one multi-variate analysis to said constructed multi-dimensional vectors comprises the steps of: reducing said constructed multi-dimensional vectors; and, applying at least one self-organizing clustering methodology to said reduced multi-dimensional vectors,

said application of said at least one self-organizing clustering methodology producing a corresponding output set of clusters.

11. The method of claim 10, wherein said establishing step comprises the steps of: loading at least one selectable metric; correlating individual ones of said clusters in said output set; determining whether any of said correlations deviate from said loaded at least one selectable metric; and, for each one of said correlated clusters in said output set which deviates from said loaded at least one selectable metric, labeling said deviating correlated cluster as exhibiting anomalous behavior.

**CERTIFICATE OF INTEREST**

Counsel for Longhorn HD LLC. certifies the following:

1. Provide the full names of all entities represented by undersigned counsel in this case:

**Longhorn HD LLC.**

2. Provide the full names of all real parties in interest (if the party named in the caption is not the real party in interest) for the entities. Do not list the real parties if they are the same as the entities:

**None/Not Applicable**

3. Provide the full names of all parent corporations for the entities and all publicly held companies that own 10 percent or more of the stock in the entities:

**Alpha Alpha Intellectual Partners LLC (Parent corporation)**

4. The names of all law firms and the partners or associates that (a) appeared for the entities in the originating court or agency or (b) are expected to appear in this court for the entities. Do not include those who have already entered an appearance in this court. Fed. Cir. R. 47.4(a)(4):

**RUBINO LAW LLC, 830 Morris Turnpike, Short Hills, NJ 07078:  
John Andrew Rubino**

**TRUELOVE LAW FIRM, PLLC, 100 West Houston Street, Marshall,  
TX 75670: Justin Kurt Truelove**

5. The following cases are pending in a court or agency and will directly affect or be directly affected by this court's decision in the pending appeal:

***Unified Patents, LLC v. Longhorn HD LLC., IPR2020-00879 (P.T.A.B.  
Nov. 9, 2021)***

6. Provide any information required under Fed. R. App. P. 26.1(b) (organizational victims in criminal cases) and 26.1(c) (bankruptcy case debtors and trustees). Fed. Cir. R. 47.4(a)(6).

**None/Not Applicable**

Dated: June 22, 2022

By: /s/ Alfred R. Fabricant  
Alfred R. Fabricant  
Fabricant LLP

**TABLE OF CONTENTS**

	<u>Page(s)</u>
PATENT CLAIMS AT ISSUE.....	i
U.S. PATENT NO. 7, 260,846 (Appx055).....	i
CERTIFICATE OF INTEREST .....	iii
STATEMENT OF RELATED CASES.....	1
JURISDICTIONAL STATEMENT .....	2
STATEMENT OF THE ISSUES .....	3
STATEMENT OF THE CASE.....	4
I.    PROCEDURAL HISTORY.....	4
II.    THE '846 PATENT.....	4
III.    THE ASSERTED PRIOR ART .....	6
A.    Portnoy '196 Provisional (U.S. Prov. Pat. App. No. 60/340,196) (Appx956).....	6
B.    Portnoy '894 Provisional (U.S. Prov. Pat. App. No. 60/352,894) (Appx1543).....	8
C.    Portnoy '966 Patent (U.S. Patent No 9,306,966) (Appx921) .....	10
SUMMARY OF THE ARGUMENT .....	12
ARGUMENT AND STANDARD OF REVIEW.....	13
IV.    STANDARD OF REVIEW .....	13
V.    THE PORTNOY '966 PATENT FAILS <i>DYNAMIC DRINKWARE</i> ANALYSIS BECAUSE IT IS NOT PATENTABLE SUBJECT MATTER UNDER SECTION 101 AND THEREFORE IS NOT PRIOR ART .....	15
VI.    CONCLUSION .....	19

CERTIFICATE OF COMPLIANCE.....21

**TABLE OF AUTHORITIES**

	<b>Page(s)</b>
<b>Cases</b>	
<i>Alice Corp. v. CLS Bank Int'l</i> , 573 U.S. 208 (2014).....	16, 17
<i>Ariad Pharms., Inc. v. Eli Lilly &amp; Co.</i> , 598 F.3d 1336 (Fed. Cir. 2010) ( <i>en banc</i> ) .....	15, 16, 17
<i>Chevron U.S.A., Inc. v. Nat. Res. Def. Council, Inc.</i> , 467 U.S. 837 (1984).....	13
<i>Cleveland Clinic Found. v. True Health Diagnostic LLC</i> , 760 F. App'x. 1013 (Fed. Cir. 2019) .....	13
<i>Consol. Edison Co. of New York v. NLRB</i> , 305 U.S. 197 (1938).....	14
<i>Dickinson v. Zurko</i> , 527 U.S. 150 (1999).....	14
<i>Dynamic Drinkware, LCC v. Nat'l Graphics, Inc.</i> , 800 F.3d 1375 (Fed. Cir. 2015) .....	<i>passim</i>
<i>In re Gartside</i> , 203 F.3d 1305 (Fed. Cir. 2000) .....	14
<i>In re Innotron Diagnostics</i> , 800 F.2d 1077 (Fed. Cir. 1986) (Markey, J.).....	13
<i>Intellectual Ventures I LLC v. Motorola Mobility LLC</i> , 870 F.3d 1320 (Fed. Cir. 2017) .....	14
<i>Mayo Collaborative Servs. v. Prometheus Labs., Inc.</i> , 566 U.S. 66 (2012).....	16
<i>Oil States Energy Servs., LLC v. Greene's Energy Grp., LLC</i> , 138 S. Ct. 1365 (2018).....	13
<i>United States v. Eurodif S.A.</i> , 555 U.S. 305 (2009).....	13

<i>United States v. Mead Corp.,</i> 533 U.S. 218 (2001).....	13
---	----

**Statutes**

35 U.S.C. § 101.....	12
35 U.S.C. § 112.....	15

**STATEMENT OF RELATED CASES**

In accordance with Federal Circuit Rule 47.5, counsel for Appellant Longhorn HD LLC. (“LHD”) states:

1. The following cases are pending and may directly affect or be directly affected by the Court’s decision in the pending appeal:

***Unified Patents, LLC. v. Longhorn HD LLC., IPR2020-00879 (P.T.A.B. Nov. 9, 2021)***

## **JURISDICTIONAL STATEMENT**

Longhorn HD LLC. appeals the Final Written Decision by the Patent Trial and Appeal Board (“Board” or “PTAB”) in the *inter partes* review (“IPR”) proceeding conducted pursuant to 35 U.S.C. §§ 6 and 318(a) for U.S. Patent No. 7,260,846 (“’846 Patent”) (IPR2020-00879). The Board issued a Final Written Decision in IPR2020-00879, dated November 9, 2021, concluding that Unified Patents, LLC had shown by a preponderance of the evidence that the following claims were unpatentable:

- (1) claims 7, 8, 10, and 11 of the ’846 Patent.

LHD filed timely a notice of appeal on January 11, 2022. This Court has subject matter jurisdiction pursuant to 35 U.S.C. § 141(c) and 28 U.S.C. § 1295(a)(4)(A).

**STATEMENT OF THE ISSUES**

1. Did the Board err by finding that the Portnoy '966 Patent is prior art under a *Dynamic Drinkware* analysis when Portnoy's invention is not patentable subject matter?

## **STATEMENT OF THE CASE**

### **I. PROCEDURAL HISTORY**

This appeal arises from IPR2020-00879 filed by Unified Patents, LLC on May 7, 2020, challenging the patentability of claims 7, 8, 10, 11 of the '846 Patent. Appx073.

On November 12, 2020, the Board instituted IPR2020-00879 with respect to claims 7, 8, 10, and 11 of the '846 Patent. Appx209. On February 12, 2021, Patent Owner conducted a deposition of Petitioner's expert, Dr. Jaideep Srivastava. Appx2275. On February 26, 2021, Patent Owner submitted Patent Owner's Response (Appx274) accompanied by the expert declaration of Mr. Zaydoon ("Jay") Jawadi (Appx2219). On June 14, 2021, Patent Owner submitted a Sur-Reply to Petitioner's Reply. Appx362. On August 25, 2021, Patent Owner participated in an Oral Hearing in front of the PTAB. Appx482. On November 9, 2021, the Board issued a Final Written Decision in IPR2020-00879 finding claims 7, 8, 10, and 11 were unpatentable. Appx001. On June 22, 2022, LHD filed this appeal. Appx566.

### **II. THE '846 PATENT**

The '846 Patent is directed to a novel Intrusion Detection System ("IDS") which overcomes prior art techniques, including primitive clustering techniques and pattern matching. For example, the '846 Patent states that a "signature" based approach or "pattern matching" are "considered to be the most primitive" because it can lead to many "false negatives." Appx65 at 2:10-19. It is noted that an enhanced

version of pattern matching, referred to as “stateful pattern matching,” which is based on a primitive form of clustering, shared the same downside. In another example regarding anomaly-based detection, the ’846 Patent states that:

Notably, though some anomaly-based analysis are configured to adapt the definition of normal state to traffic patterns as they unfold, none have been able to properly avoid the classification of some abnormal behavior as normal behavior. Moreover, no one conventional anomaly-based analysis has been able to distinguish anomalous behavior from permissible deviations from the normal state.

Appx066 at 3:5-12.

The ’846 Patent states that in order for an “effective statistical analysis, which is required to minimize false positives in the application of an anomaly based detection scheme, a maximum amount of data samples of exceptional granularity will be required.” *Id.* at 3:60-64. This approach is very resource intensive, and instead proposes a relational database, which stores data regarding multiple aspects of a packets passing across a “coupled communication path,” noting that the IDS:

can identify protocol boundaries separating the various fields of each passing network packet and can store data for selected ones or all of the fields in a database, such as a relational database. In particular, data for each field can be stored in a separate record to facilitate the robust analysis of the stored data at a substantially granular level.

*Id.* at 4:29-33.

The '846 Patent further notes that “at least one self-organizing clustering module can be configured to process the multi-dimensional vectors to produce a self-organized map of clusters” and that an “anomaly detector” can detect anomalous correlations between individual ones of the cluster in the “self-organized map.” *Id.* at 4:52-59.

The '846 Patent describes a real-world working invention capable of monitoring live network traffic, analyzing that traffic to produce output sets of data, establishing a correlation between the output sets to identify anomalous behavior, and then further classifying that anomalous behavior. This is a much more rigorous analysis of the data than in prior art, and certainly is far more advanced than Portnoy’s rudimentary academic exercise that does not even describe a functioning system.

### **III. THE ASSERTED PRIOR ART**

#### **A. Portnoy '196 Provisional (U.S. Prov. Pat. App. No. 60/340,196) (Appx956)**

The Portnoy '196 Provisional is a Columbia University article titled “Intrusion Detection with Unlabeled Data Using Clustering.” The purpose of the Portnoy '196 Provisional was to “present a new type of clustering-based intrusion detection algorithm, unsupervised anomaly detection.” Appx956. The Portnoy '196 Provisional is based on basic, prior-art clustering, does not describe the monitoring of data, the extraction and storing of data, or the use of a real dataset.

The original goal of the Portnoy '196 Provisional was to use data from the KDD CUP 1999 dataset. Appx958. The KDD CUP 1999 dataset consists of approximately 4,900,000 data instances and includes intrusions that were simulated in a military network environment. Appx959. Presumably, the KDD CUP dataset was obtained from KDD CUP through the Internet, from media (e.g., CD), or using some other manual mechanism. Appx2232, ¶ 38.

The Portnoy '196 Provisional experiment was not able to successfully use the raw KDD CUP 1999 dataset. Appx962. Using raw data, the experiment “obtained very poor performance.” *Id.* Because the 1999 KDD CUP dataset contained a simulated attack with normal activity in the background, the proportion of attack instances to normal ones in the KDD training dataset is very large as compared to the data that would be observed in a normal, real-life, system. *Id.*; Appx2233, ¶ 40.

Instead, in order for the Portnoy '196 Provisional experiment to be operational, the KDD CUP dataset had to be altered by “filtering it for attacks.” Appx962. It was “filtered such that the resulting training set consisted of 1 to 1.5% attack and 98.5 to 99% normal instances.” *Id.* The experiment disclosed by the Portnoy '196 Provisional did not work with the actual KDD CUP dataset and had to be modified to represent 1-1.5% attack activity in order to produce coherent output. Appx2233, ¶ 42.

Lastly, the '196 Portnoy Provisional contains no mention of using an audit

stream, packing sniffing, packet parsing, or any other type of real time monitoring. The testimony of Dr. Srivastava confirms this. *See* Appx2421 at 11-15 (“Q: Does Exhibit 1005 [the Portnoy ’196 Provisional] discuss any sort of monitoring tool? A: Exhibit 1005 [the Portnoy ’196 Provisional]. No, I don’t see Exhibit 1005 [the Portnoy ’196 Provisional] talking about a monitoring tool.”)

**B. Portnoy ’894 Provisional (U.S. Prov. Pat. App. No. 60/352,894) (Appx1543)**

The Portnoy ’894 Provisional is titled “A Geometric Framework for Unsupervised Anomaly Detection: Detecting Intrusions in Unlabeled Data.” Appx1543. As in the Portnoy ’196 Provisional, the Portnoy ’894 Provisional describes “a new geometric framework for unsupervised anomaly detection, which are algorithms that are designed to process unlabeled data.” *Id.* The Portnoy ’894 Provisional presents “three algorithms for detecting which points lie in sparse regions of the feature space.” *Id.* The Portnoy ’894 Provisional further describes evaluating its approach “by performing experiments over network records from the KDD CUP 1999 data set and system call traces from the 1999 Lincoln Labs DARPA evaluation.” *Id.*

Like the Portnoy ’196 Provisional, the Portnoy ’894 Provisional does not disclose a working system. Appx2236, ¶ 50. It does not describe the monitoring of data, the extraction and storing of data, or the use of a real dataset. *Id.* The Portnoy ’894 Provisional appears to have used the same altered version of the KDD CUP

dataset used by the Portnoy '196 Provisional. *See* Appx1556. (“As a result, the proportion of attack instances to normal ones in the KDD training data set is very large as compared to data that we would expect to observe in practice. . .we filtered many of the attacks so that the resulting data set consisted of 1 to 1.5% attack and 98.5 to 99% normal instances”); Appx2236, ¶ 51.

The Portnoy '894 Provisional also uses system call data from a portion of the 1999 DARPA Intrusion Detection Evaluation data. The data used for this experiment was pre-selected and consisted of “three weeks of traces of the programs which were attacked during that time. The programs we examined were *eject*, and *ps*.”). Appx1556. As in the Portnoy '196 Provisional, presumably the DARPA dataset was obtained from DARPA through the Internet, from media (e.g., CD), or using some other manual mechanism. In other words, the Portnoy experiment did not generate the DARPA dataset; instead, the DARPA dataset was simply acquired from a third party (e.g., DARPA). Appx2236, ¶ 52.

Moreover, the Portnoy '894 Provisional describes the DARPA dataset as “system call traces from the 1999 Lincoln Labs DARPA evaluation,” “system call data set was obtained from the 1999 Lincoln Labs,” and “system call data is from the BSM (Basic Security Module) data portion of the 1999 DARPA Intrusion Detection Evaluation data created by MIT Lincoln Labs.” Appx1543, Appx1546, Appx1556 (emphasis added). In other words, the DARPA dataset consists of system

call traces / data, not packets. A POSITA would not conflate system calls and packets. Appx2236-2237, ¶ 53. A POSITA would understand that system calls are not collected using network monitoring. *Id.* Therefore, the DARPA dataset does not disclose or imply monitoring network traffic passing across a network communication path. *Id.*

Furthermore, the Portnoy '894 Provisional does not disclose a packet sniffer or any tool used to monitor a network stream to collect data. Appx2237, ¶ 54. This was corroborated by Dr. Srivastava who admitted that the Portnoy '894 Provisional does not contain a packet sniffer. Appx2421 at 6-10 (“Q: Does it contain a packet sniffer? A: You mean, Exhibit 1007 does not talk about a packet sniffer, no.”) Dr. Srivastava also states that the Portnoy '894 Provisional does not disclose an “operational system.” (“Q: What do you mean by real world system? A: Operational system. One that is in this particular context one that is actually operationally deployed. Q: So, Portnoy does not expressly disclose an operation system, right? A: At least not in exhibits 1005 and 1007 that we just discussed.”). Appx2422 at 13-21.

### **C. Portnoy '966 Patent (U.S. Patent No 9,306,966) (Appx921)**

The Portnoy '966 Patent is titled “Methods of Unsupervised Anomaly Detection Using A Geometric Framework.” One of the objects of the Portnoy '966 Patent is to “provide a technique for detecting anomalies in the operation of a computer system which implicitly maps audit data in a feature space, and which

identifies anomalies based on the distribution of data in feature space.” *Id.* at 4:42-46.

The ’966 Patent contains no discussions of data reduction, stream monitoring, or the manner or type of data which needs to be stored. Instead, the ’966 Patent disclosure is limited to training for and detecting anomalies from unlabeled data in an unsupervised environment which would “operate[] in an efficient manner for a large volume of data.” Appx941at 4:47-49.

Unlike the ’194 and ’894 Portnoy Provisionals, the specification of the ’966 Patent briefly discusses collection of data. However, such discussion is limited to a rudimentary form of data collection, where all parts of a TCP packet are sniffed then mapped into vector space using a “tcpdump.” Appx934 at 8:22-28. Aside from this disclosure, the ’966 Patent is silent with regard to how to monitor, parse, and store the data in a packet.

The ’966 Patent describes routine steps applied to an abstract idea. For example, Claim 1 recites:

1. A method for unsupervised detection of an anomaly in the operation of a computer system comprising:
  - (b) mapping a set of unlabeled data instances, which do not indicate any anomaly occurrence, to a feature space;
  - (c) calculating one or more sparse regions in the feature space; and
  - (d) designating one or more data instances from the set of unlabeled data instances as an anomaly if said one or more

data instances is located in said one or more sparse regions of the feature space.

Appx954 at 29:26-35.

Just as the Portnoy Provisionals discussed above do not detail a real-world working system, the Portnoy '966 Patent merely describes an abstract idea. The steps of mapping, calculating, and designating are nothing more than routine data manipulation procedures.

### **SUMMARY OF THE ARGUMENT**

The Board's Final Written Decision concluding that the '846 Patent is unpatentable in view of the Portnoy '966 Patent should be reversed and vacated.

The Board erred when it considered Portnoy to be valid prior art under a *Dynamic Drinkware* analysis, despite acknowledging Claim 1 of Portnoy is likely unpatentable subject matter under a 35 U.S.C. § 101 analysis. Petitioner asserts the Portnoy '966 Patent should be afforded the filing date of its provisionals based on pre-AIA section 102(e). However, pre-AIA section 102(e) and analysis under *Dynamic Drinkware* focuses on **invention**. Claim 1 of the Portnoy '966 Patent (which Petitioner relies upon) is not an invention under a section 101 analysis and therefore cannot be prior art under pre-AIA section 102(e) and the *Dynamic Drinkware* analysis.

## **ARGUMENT AND STANDARD OF REVIEW**

### **IV. STANDARD OF REVIEW**

When reviewing the Board's decision, the Federal Circuit assesses the Board's compliance with governing legal standards *de novo* and its underlying factual determinations for substantial evidence. *Oil States Energy Servs., LLC v. Greene's Energy Grp., LLC*, 138 S. Ct. 1365, 1372 (2018).

The PTO's statutory interpretation is analyzed under *Chevron U.S.A., Inc. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837 (1984). *Chevron* requires a court reviewing an agency's construction of a statute it administers to determine first "whether Congress has directly spoken to the precise question at issue." 467 U.S. at 842. If yes, the inquiry ends, and effect is given to Congress's unambiguous intent. *Id.* at 842–43. If the answer is no, the court must consider "whether the agency's answer [to the precise question at issue] is based on a permissible construction of the statute." *Id.* at 843. The agency's "interpretation governs in the absence of unambiguous statutory language to the contrary or unreasonable resolution of language that is ambiguous." *United States v. Eurodif S.A.*, 555 U.S. 305, 316 (2009) (citing *United States v. Mead Corp.*, 533 U.S. 218, 229–30 (2001)).

The Federal Circuit is the primary authority (aside from the Supreme Court) on issues of substantive patent law. *Cleveland Clinic Found. v. True Health Diagnostic LLC*, 760 F. App'x. 1013, 1020 (Fed. Cir. 2019) (nonprecedential)

(“While we greatly respect the PTO’s expertise on all matters relating to patentability, including patent eligibility, we are not bound by its guidance.”); *In re Innotron Diagnostics*, 800 F.2d 1077, 1084 (Fed. Cir. 1986) (Markey, J.) (discussing “the congressionally envisioned role of this court, *i.e.*, to contribute to doctrinal stability in the field of patent law”).

This Court *reviews* factual findings for substantial evidence. The Board’s finding is supported by substantial evidence if a reasonable mind might accept the evidence as adequate to support the finding. *Consol. Edison Co. of New York v. NLRB*, 305 U.S. 197, 229 (1938). The substantial evidence standard asks “whether a reasonable fact finder could have arrived at the agency’s decision,” and “involves examination of the record as a whole, taking into account evidence that both justifies and detracts from an agency’s decision.” *In re Gartside*, 203 F.3d 1305, 1312 (Fed. Cir. 2000). The Supreme Court “has stressed the importance of not simply rubber-stamping agency factfinding . . . The [Administrative Procedure Act] requires meaningful review; and its enactment meant stricter judicial review of agency factfinding than Congress believed some courts had previously conducted.” *Dickinson v. Zurko*, 527 U.S. 150, 162 (1999).

“Mere speculation” is not substantial evidence. *See Intellectual Ventures I LLC v. Motorola Mobility LLC*, 870 F.3d 1320, 1331 (Fed. Cir. 2017).

**V. THE PORTNOY '966 PATENT FAILS *DYNAMIC DRINKWARE* ANALYSIS BECAUSE IT IS NOT PATENTABLE SUBJECT MATTER UNDER SECTION 101 AND THEREFORE IS NOT PRIOR ART**

Petitioner relies on Claim 1 of the Portnoy '966 Patent for alleged support of its *Dynamic Drinkware* analysis. However Claim 1 of Portnoy is directed to nothing more than an abstract idea and is not patentable. Because Claim 1 of Portnoy is not a patentable invention, the '966 Patent cannot claim priority to an earlier provisional date.

U.S. Patents have effective prior art dates under pre-AIA § 102(e) based on the filing date of an underlying provisional application only if (1) the subject matter relied upon in the patent is described in the provisional application, and (2) at least one of the issued claims is supported by the written description of the provisional application in compliance with pre-AIA 35 U.S.C. § 112, first paragraph. *Dynamic Drinkware, LCC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

The test for determining compliance with the written description requirement is whether the original disclosure of the patent application reasonably conveys to a person of ordinary skill in the art that the inventor had possession of the claimed subject matter as of the filing date. *Ariad Pharm., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (*en banc*).

Ariad further states:

Patents are not awarded for academic theories, no matter how groundbreaking or necessary to the later patentable inventions of others. “[A] patent is not a hunting license. It is not a reward for the search, but compensation for its successful conclusion.” *Id.* at 930 n. 10 (quoting *Brenner*, 383 U.S. at 536, 86 S. Ct. 1033). Requiring a written description of the invention limits patent protection to those who actually perform the difficult work of “invention”—that is, conceive of the complete and final invention with all its claimed limitations—and disclose the fruits of that effort to the public.

*Id.* at 1353. Thus, the claims of the alleged reference must be directed to inventive subject matter in order to provide support for an analysis under *Dynamic Drinkware*. Whether or not claims are directed to patentable subject matter is analyzed in a two-step framework. *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 217, (2014); *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 70–73 (2012). First, one must ascertain whether a patent claim is directed to an unpatentable law of nature, natural phenomenon, or abstract idea. *Alice Corp.*, 573 U.S. at 217. If so, one next must determine whether the claim nonetheless includes an “inventive concept” sufficient to “transform the nature of the claim’ into a patent-eligible application.” *Id.* (quoting *Mayo*, 566 U.S. at 72, 78).

Claim 1 of Portnoy recites:

1. A method for unsupervised detection of an anomaly in the operation of a computer system comprising:
  - (b) mapping a set of unlabeled data instances, which do not indicate any anomaly occurrence, to a feature space;
  - (c) calculating one or more sparse regions in the feature space; and
  - (d) designating one or more data instances from the set of unlabeled data instances as an anomaly if said one or more data instances is located in said one or more sparse regions of the feature space.

Appx954 at 29:26-35.

Nothing in the claim indicates that these steps must even be done by a computer. In fact, the data analyzed by Portnoy was manufactured by Portnoy, not by a computer system. Appx962, section 3.2. This claim is an abstract idea with subsequent data manipulation steps. Applying step 2 of the *Alice* analysis, the limitations of mapping, calculating, and designating are routine steps that are not entitled to patent protection. The Board even described Claim 1 as simply a set of data manipulation steps (“[b]ut on the merits, it does look like the Portnoy claim is just sort of data manipulation of claim 1.”). Appx502 at 7-8. As such, the Portnoy '966 Patent, and Claim 1, are merely directed to academic theories. *Alice Corp.*, 573 U.S. at 217 (2014). As the Federal Circuit stated in *Ariad*, “[p]atents are not awarded for academic theories, no matter how groundbreaking or necessary to the later patentable inventions of others.” *Ariad Pharms.*, 598 F.3d at 1353.

Petitioner and the Board misconstrue Patent Owner's analysis by stating that "there is no known precedent requiring consideration of patent subject matter eligibility for determining prior art eligibility," stating that §102(e) can be directed both at a patent and a patent application. Appx344, Appx019. However, the *Dynamic Drinkware* analysis requires a ***claimed invention*** ruling that, "[a] reference patent is only entitled to claim the benefit of the filing date of its provisional application if the disclosure of the provisional application provides support for the claims in the reference patent in compliance with §112 ¶1." See *Dynamic Drinkware*, 800 F.3d at 1381 (citation omitted). *Dynamic Drinkware* applies only to pre-AIA 102(e), which focused on the ***invention*** of another, not merely a ***disclosure*** as in pre-AIA 102(a) and 102(b). Accordingly, in order to perform *Dynamic Drinkware* analysis, there must be an ***invention*** and a patent claim to that patentable subject matter. As shown, Portnoy relies on a disclosure that is *not* an invention and thus, unpatentable subject matter.

Further, public policy favors an interpretation of pre-AIA section 102(e) that requires an invalidating patent to be valid itself. As discussed above, a patent is required to "carry through" the disclosures in the provisional application under the written description requirement of section 112 in order to be afforded the filing date of the provisional. It would be incongruous to make such a substantive requirement of a patent in order for it to receive the benefit of an earlier filing date, and then ignore

the most important and substantive aspect of the patent—whether it even claims patentable subject matter. The instant case is a clear example of this failure of interpretation and displays the absurdity of the result: a patent that even the Board commented is likely not patentable subject matter can be used to invalidate an otherwise valid patent.

Because claim 1 of the '966 Patent is not directed to patentable subject matter, it is not a claimed invention and fails *Dynamic Drinkware* analysis. Accordingly, Portnoy is, therefore, not entitled to its provisional filing date and is not prior art. Without Portnoy, the Petition fails to demonstrate that any of the challenged claims are invalid.

## VI. CONCLUSION

For the foregoing reasons, LHD respectfully requests that the Court reverse and vacate the Board's Final Written Decision finding unpatentable claims 7, 8, 10, and 11 of the '846 Patent.

Dated: June 22, 2022

Respectfully submitted,

/s/ Alfred R. Fabricant

Alfred R. Fabricant

Peter Lambrianakos

Vincent J. Rubino, III

Enrique W. Iturralde

**FABRICANT LLP**

411 Theodore Fremd Avenue,

Suite 206 South

Rye, New York 10580

Telephone: (212) 257-5797

Facsimile: (212) 257-5796

*Attorneys for Appellant  
Longhorn HD LLC.*

**CERTIFICATE OF COMPLIANCE**

I certify that this Brief complies with the type-volume limitation of Fed. R. App. P. 27(d)(2)(A). This Brief contains 3,796 words, excluding the parts exempted by Fed. R. App. 27(d) and Fed. Cir. R. 27(d). This Brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the typestyle requirements of Fed. R. App. 32(a)(6). This Brief has been prepared in a proportionally spaced typeface using Microsoft Word for Office 365 in 14-point Times New Roman font.

Dated: June 22, 2022

Respectfully submitted,

/s/ Alfred R. Fabricant

Alfred R. Fabricant  
Peter Lambrianakos  
Vincent J. Rubino, III  
Enrique W. Iturralde  
**FABRICANT LLP**  
411 Theodore Fremd Avenue,  
Suite 206 South  
Rye, New York 10580  
Telephone: (212) 257-5797  
Facsimile: (212) 257-5796

*Attorneys for Appellant  
Longhorn HD LLC.*

**CERTIFICATE OF SERVICE**

I hereby certify that I caused to be electronically filed the foregoing Appellant's Principal and Opening Brief with the Clerk of the Court for the United States Court of Appeals for the Federal Circuit by using the appellate CM/ECF system on June 22, 2022 and thus caused to be served on all registered counsel of record a copy of the same via the CM/ECF system.

Dated: June 22, 2022

/s/ Alfred R. Fabricant  
Alfred R. Fabricant

# ADDENDUM

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

UNIFIED PATENTS, LLC,  
Petitioner,

v.

LONGHORN HD LLC,  
Patent Owner.

---

IPR2020-00879  
Patent 7,260,846 B2

---

Before KARL D. EASTHOM, GARTH D. BAER, and  
MATTHEW S. MEYERS, *Administrative Patent Judges*.

MEYERS, *Administrative Patent Judge*.

JUDGMENT  
Final Written Decision  
Determining All Challenged Claims Unpatentable  
*35 U.S.C. § 318(a)*  
Dismissing Petitioner's Motion to Exclude  
*37 C.F.R. § 42.64*

## I. INTRODUCTION

### *A. Background and Summary*

Unified Patents, LLC, (“Petitioner”) filed a Petition (Paper 1, “Petition” or “Pet.”) requesting *inter partes* review of claims 7, 8, 10, and 11 of U.S. Patent No. 7,260,846 B2 (Ex. 1001, “the ’846 patent”). Longhorn HD LLC, (“Patent Owner”) filed a Preliminary Response. Paper 8. We instituted an *inter partes* review on claims 7, 8, 10, and 11 on all grounds asserted in the Petition. *See* Paper 10 (“Decision on Institution” or “Dec. on Inst.”). After institution of trial, Patent Owner filed a Patent Owner Response (Paper 15, “PO Resp.”), Petitioner filed a Reply (Paper 18, “Pet. Reply”), and Patent Owner filed a Sur-Reply (Paper 20, “Sur-Reply”).

After filing an objection to Patent Owner’s evidence (Paper 16), Petitioner filed a motion to exclude certain testimony from the declaration of Mr. Jawadi. Paper 24 (“Mot.”). Patent Owner filed an opposition (Paper 25, “Opp.”), and Petitioner filed a reply (Paper 26, “Reply”). We held a hearing on August 25, 2021, a transcript of which is included in the record. *See* Paper 33 (“Tr.”).

We have authority under 35 U.S.C. § 6. Petitioner bears the burden of proving unpatentability of the challenged claims, and the burden of persuasion never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). To prevail, Petitioner must prove unpatentability by a preponderance of the evidence. *See* 35 U.S.C. § 316(e) (2018); 37 C.F.R. § 42.1(d) (2019). This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons discussed below, we determine that Petitioner has shown by a preponderance of the evidence that claims 7, 8, 10, and 11 of the ’846 patent are unpatentable.

### *B. Real Parties in Interest*

Unified Patents indicates that it alone is the real party-in-interest, and that “no other party exercised control or could have exercised control over Unified’s participation in this proceeding, the filing of this petition, or the conduct of any ensuing trial.” Pet. 1. Patent Owner indicates that it alone is the real party-in-interest. Paper 4, 2.

### *C. Related Matters*

Petitioner identifies the following district court proceedings as related to the ’846 patent: *Longhorn HD LLC. v. Fortinet Inc.*, 2:19-cv-00124 (E.D. Tex. April 16, 2019); *Longhorn HD LLC. v. Juniper Networks, Inc.*, 2:19-cv-00385 (E.D. Tex. Nov. 20, 2019); and *Longhorn HD LLC. v. Check Point Software Technologies Ltd.*, No. 2:19-cv-00384 (E.D. Tex. Nov. 11, 2019). Pet. 2.

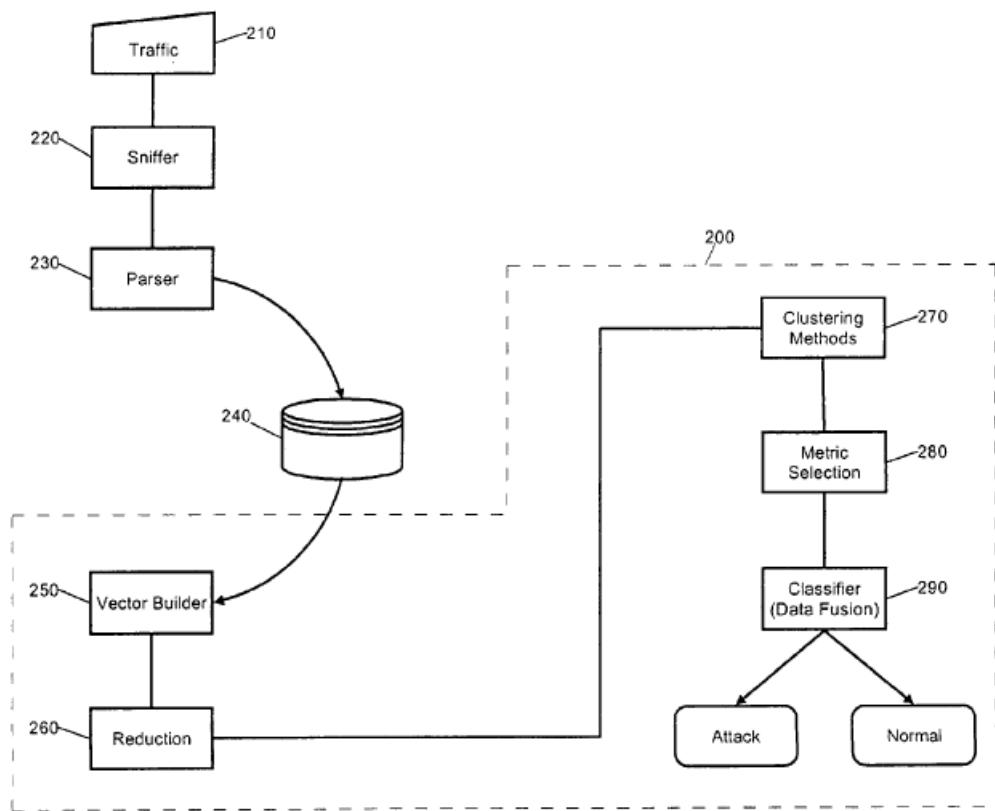
## II. BACKGROUND

### *A. The ’846 Patent*

The ’846 patent is titled “INTRUSION DETECTION SYSTEM.” Ex. 1001, code (54). According to the ’846 patent, “[t]o fill the security gap left open by firewall usage, information technologists incorporate intrusion detection system (IDS) technology within the enterprise.” *Id.* at 1:44–46. The ’846 patent is directed to an IDS that “can monitor [any] packets passing across a coupled communications path” and “identify protocol boundaries separating the various fields of each passing network packet and can store data for selected ones or all of the fields in a database, such as a relational database.” *Id.* at 4:25–31. “In particular, data for each field can be stored in a separate record to facilitate the robust analysis of the stored data at a substantially granular level.” *Id.* at 4:31–33.

The '846 patent explains that “[o]nce sufficient data has be[en] stored in the database, multidimensional vectors can be constructed and reduced from the stored data” and “[t]he reduced multi-dimensional vectors can be processed using one or more conventional multi-variate analysis methods and the output sets produced by the multi-variate analysis methods can be correlated against one another according to one or more selected metrics.” Ex. 1001, 4:34–40. Then, “[b]ased upon these correlations, both normal and anomalous events can be identified.” *Id.* at 4:40–42.

Figure 2 of the '846 patent, reproduced below, is a flow chart illustrating a process for performing intrusion detection. Ex. 1001, 8:6–7.



As shown in Figure 2 (above), packet sniffer 220 can extract network traffic 210 flowing across a communications path coupled to IDS 200. *Id.* at 8:7–10. Parser 230 can de-construct the network packets along known protocol field boundaries, such as destination and source IP address, time-to-live,

IPR2020-00879

Patent 7,260,846 B2

payload size, packet type, type of service, etc. *Id.* at 8:28–31. Subsequently, selected ones of the de-constructed fields can be stored in separate records in database 240 and can be associated with the particular socket to which the packet belongs. *Id.* at 8:32–35.

In block 250, a vector builder in a feature extraction process can select individual ones of the network packet fields to be included in the construction of a multi-dimensional vector. Ex. 1001, 8:39–42. Multi-dimensional vectors can be constructed using the chosen features produced in block 250. *Id.* at 8:51–53. Specifically, the vector builder can process the records in the database 240 to identify pertinent fields associated with a particular “conversation” or socket. *Id.* at 8:53–55. In block 260, a vector separation system can reduce the dimensionality of the multi-dimensional vectors in order to simplify a subsequent multi-variate analysis. *Id.* at 8:64–66. Components of the multi-dimensional vectors that appear to be redundant, irrelevant, or otherwise insignificant relative to other interested components can be eliminated across all or a selection of the multi-dimensional vectors to produce a set of reduced vectors. *Id.* at 8:66–9:7.

In block 270, one or more self-organizing clustering methodologies can be applied concurrently or sequentially to the set of reduced vectors. Ex. 1001, 9:8–10. After the reduced vectors have been processed by the multiple clustering methodologies in block 270, one or more metrics can be selected in block 280 for purposes of establishing a correlation between the output sets of the processed reduced multi-dimensional vectors. *Id.* at 9:15–19. In block 290 a classifier can identify from any established correlations whether an anomaly has been detected. *Id.* at 9:21–23. The classification process of block 290 can identify either normal traffic or an attack. *Id.* at 9:25–26.

*B. Illustrative Claims*

The '846 patent includes twelve claims, and Petitioner challenges claims 7, 8, 10, and 11. Claim 7, the sole challenged independent claim, is illustrative and reads as follows:

1. An intrusion detection method comprising the steps of:
  - monitoring network traffic passing across a network communications path;
  - extracting network packets from said passing traffic;
  - storing individual components of said network packets in a database;
  - constructing multi-dimensional vectors from at least two of said stored individual components and applying at least one multi-variate analysis to said constructed multi-dimensional vectors, said at least one multi-variate analysis producing a corresponding output set;
  - establishing a correlation between individual output sets based upon a selected metric to identify anomalous behavior; and
  - classifying said anomalous behavior as an event selected from the group consisting of a network fault, a change in network performance and a network attack.

Ex. 1001, 11:29–45.

*C. Asserted Grounds of Unpatentability*

Pursuant to 35 U.S.C. § 314(a), on November 11, 2020, we instituted *inter partes* review on all grounds asserted in the Petition, namely:

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
7, 8	103(a) <sup>1</sup>	Portnoy, <sup>2</sup> Cannady, <sup>3</sup> Barbara <sup>4</sup>
10, 11	103(a)	Portnoy, Cannady, Barbara, AAPA

*See* Pet. 4, 5, 29–70. Petitioner also relies on the declaration of Jaideep Srivastava, Ph.D. Ex. 1002 (“Srivastava Decl.”). Patent Owner relies on testimony from Zaydoon Jawadi. Ex. 2001 (“Jawadi Decl.”).<sup>5</sup> Patent Owner cross-examined Dr. Srivastava. *See* Ex. 2003 (deposition transcript of Dr. Jaideep Srivastava, “Srivastava Dep.”).

### III. ANALYSIS

#### A. *Principles of Law*

To prevail in its challenges to Patent Owner’s claims, Petitioner must demonstrate by a preponderance of the evidence that the challenged claims are unpatentable. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d) (2019). A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between

---

<sup>1</sup> The relevant sections of the Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112–29, took effect on March 16, 2013. Because the application that issued as the ’351 patent was filed before March 16, 2013, we apply the pre-AIA version of § 103.

<sup>2</sup> Eskin et al., US 9,306,966 B2, issued Apr. 5, 2016 (Ex. 1004). Petitioner and Patent Owner both refer to this reference as “Portnoy.” Accordingly, this Decision also refers to Exhibit 1004 as Portnoy.

<sup>3</sup> Cannady, J., “*Artificial Neural Networks for Misuse Detection*,” Nova Southeastern University School of Computer and Information Sciences (Ex. 1012). *See* Pet. 16 (“Cannady was publicly accessible by December 10, 1998 and May 20, 1999 at the Cornell University Library.”).

<sup>4</sup> Barbara, D., “*Detecting Novel Network Intrusions Using Bayes Estimators*,” First SIAM International Conference on Data Mining conference (April 2001) (Ex. 1013).

<sup>5</sup> We note that many of Patent Owner’s citations to Mr. Jawadi’s declaration refer to the wrong paragraph. We understand this to be typographical error, and our analysis refers to the intended paragraph when providing citation.

IPR2020-00879

Patent 7,260,846 B2

the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.

*KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) when in evidence, objective evidence of non-obviousness.<sup>6</sup> *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

#### *B. Level of Ordinary Skill in the Art*

We review the grounds of unpatentability in view of the understanding of a person of ordinary skill in the art at the time of invention. *Graham*, 383 U.S. at 17. Petitioner asserts that a person having ordinary skill in the art at the time of the invention (“POSITA”) would have had “(i) a Bachelor of Science in Electrical and Computer Engineering, Mathematics, Computer Science, or the equivalent, and (ii) approximately two years of experience with network security and intrusion detection related fields.” Pet. 28–29 (citing Ex. 1002 ¶ 45). Patent Owner does not dispute Petitioner’s assessment or otherwise argue that that it would affect the merits of the case. *See generally* PO Resp.

We adopt the assessment offered by Petitioner as it is consistent with the ’846 patent and the asserted prior art. The prior art of record in the instant proceeding reflects the appropriate level of ordinary skill in the art.

---

<sup>6</sup> Patent Owner presents no evidence of objective indicia in its papers. *See generally* PO Resp.; PO Sur-Reply.

*Cf. Okajima v. Bourdeau*, 261 F.3d 1350, 1354–55 (Fed. Cir. 2001) (the prior art itself may reflect an appropriate level of skill in the art).

### C. Claim Construction

In an *inter partes* review for a petition filed on or after November 13, 2018, “[claims] of a patent . . . shall be construed using the same claim construction standard that would be used to construe the [claims] in a civil action under 35 U.S.C. 282(b), including construing the [claims] in accordance with the ordinary and customary meaning of such [claims] as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” *See* 37 C.F.R. § 42.100(b); *see also Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005) (en banc). “In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1015, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17).

According to Petitioner, “a POSITA would apply the ordinary and customary meanings to all the claim elements in the challenged claims of the ’846 patent,” and as such, “no specific claim construction is necessary.” Pet. 29. Patent Owner does not dispute Petitioner’s assessment. *See generally* PO Resp; *see also* Ex. 2001 ¶ 30 (“Although I am not rendering an opinion regarding claim construction, my opinions and analysis apply to Petitioner’s proposed meanings of the claim terms.”).

We determine, as we did in the Institution Decision, that no explicit construction of claim terms is needed to resolve the issues presented by the arguments and evidence of record. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (per curiam)

IPR2020-00879

Patent 7,260,846 B2

(claim terms need to be construed “only to the extent necessary to resolve the controversy” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

*D. Alleged Obviousness over Portnoy, Cannady, and Barbara  
(Ground 1: Claims 7 and 8)*

Petitioner contends that claims 7 and 8 are unpatentable as obvious over Portnoy, Cannady, and Barbara. Pet. 30–60. Petitioner also relies on the testimony of Dr. Srivastava to support its arguments. *Id.* Patent Owner disagrees with Petitioner’s assertions. PO. Resp. 4–32; Sur-Reply 2–12. Patent Owner relies on the testimony of Mr. Jawadi to support its arguments. *Id.*

We begin our discussion with a brief summary of Portnoy, Cannady, and Barbara and then address the evidence and arguments presented.

*1. Overview of Portnoy (Ex. 1004)*

Portnoy “relates to systems and methods [for] detecting anomalies in the operation of a computer system, and more particularly to a method of unsupervised anomaly detection.” Ex. 1004, 1:49–51. By way of background, Portnoy explains that the most widely deployed and commercially available methods for intrusion detection employ signature-based detection. *Id.* at 1:55–57. Signature-based detection methods extract features from various audit streams, and detect intrusions by comparing the feature values to a set of known attack signatures provided by human experts. *Id.* at 1:57–60. Signature-based detection methods can only detect previously known intrusions, the signature database has to be manually revised for each new type of attack that is discovered, and, until this revision, systems are vulnerable to these attacks. *Id.* at 1:60–64.

IPR2020-00879

Patent 7,260,846 B2

Portnoy explains that another approach to intrusion detection is supervised anomaly detection. Ex. 1004, 2:40–41. Some supervised anomaly detection systems may be considered to perform “generative modeling,” which involves building a model over the normal data and then checking to see how well new data fits into that model. *Id.* at 2:42–45. A limitation of supervised anomaly detection algorithms, however, is that they require a set of purely normal data from which they train their model, but labeled or purely normal data may not be readily available, or may be prohibitively expensive. *Id.* at 3:6–16.

Portnoy further describes “a third paradigm of intrusion detection algorithms” that is known as “unsupervised anomaly detection.” Ex. 1004, 3:28–29. According to Portnoy, unsupervised anomaly detection has many advantages over supervised anomaly detection systems. *Id.* at 3:50–51. One advantage is that unsupervised anomaly detection does not require a purely normal training set. *Id.* at 3:51–52. Unsupervised anomaly detection algorithms can be performed over unlabeled data, which is typically easier to obtain because it is simply raw audit data collected from a system. *Id.* at 3:53–56. Portnoy describes “a system and methods for detecting an intrusion in the operation of a computer system comprising receiving a set of data corresponding to a computer operation and having a set or vector of features.” *Id.* at 4:52–55. And because the method is an unsupervised anomaly detection method, the set of data to be analyzed need not be labeled to indicate an occurrence of an intrusion or an anomaly. *Id.* at 4:55–58. The method implicitly maps the set of data instances to a feature space, and determines a sparse region in the feature space. *Id.* at 4:58–60. A data instance is designated as an anomaly if it lies in the sparse region of the feature space. *Id.* at 4:60–61.

## 2. Whether Portnoy Qualifies as Prior Art

The parties dispute whether Portnoy (also referred to as the Portnoy patent) qualifies as prior art to the '846 patent.<sup>7</sup> Petitioner asserts that Portnoy qualifies as prior art under (pre-AIA) 35 U.S.C. § 102(e) because it is entitled to the priority dates of its provisional applications, which were filed on December 14, 2001,<sup>8</sup> and January 29, 2002,<sup>9</sup> respectively. Pet. 3, 9–15; Pet. Reply 1–16. Patent Owner disagrees and argues that Petitioner failed to meet its burden to properly establish that Portnoy is entitled to the earlier priority date of its provisional applications under the standard set forth by the Federal Circuit in *Dynamic Drinkware*. PO Resp. 13 (citing *Dynamic Drinkware*, 800 F.3d at 1378–80); *see also id.* at 13–22.

The Federal Circuit in *Dynamic Drinkware* began with the requirement that a patent must satisfy 35 U.S.C. § 119(e)(1) to gain the benefit of a provisional application filing date. *Dynamic Drinkware*, 800 F.3d at 1378. According to the Federal Circuit, this requirement includes that “the specification of the provisional must ‘contain a written description of the invention . . . in such full, clear, concise, and exact terms,’ . . . to enable an ordinarily skilled artisan to practice the invention claimed in the non-provisional application.” *New Railhead Mfg., L.L.C. v. Vermeer Mfg. Co.*, 298 F.3d 1290, 1294 (Fed. Cir. 2002) (quoting 35 U.S.C. § 112, first

---

<sup>7</sup> For prior art purposes, “Petitioner assumes a priority date [of] July 30, 2002” for the '846 patent. Pet. 6, fn. 3. Patent Owner agrees with this assessment. *See* PO Resp. 1–2 (“[T]he earliest filing date of the '846 Patent . . . [is] July 30, 2002.”).

<sup>8</sup> U.S. Provisional Patent Application No. 60/340,196, filed Dec. 14, 2001 (Ex. 1005) (“Portnoy '196 Provisional”).

<sup>9</sup> U.S. Provisional Patent Application No. 60/352,894, filed Jan. 29, 2002 (Ex. 1007) (“Portnoy '894 Provisional”).

IPR2020-00879

Patent 7,260,846 B2

paragraph) (*quoted in Dynamic Drinkware*, 800 F.3d at 1378) (emphasis omitted).

Of particular note is the focus on “the *invention* claimed” in the non-provisional application (later issued as the reference patent). *New Railhead*, 298 F.3d at 1294 (emphasis added and omitted). This is consistent with prior Federal-Circuit precedent explaining that the rationale behind § 102(e) is that a patent should be “treated as prior art as of its filing date because at the time the application was filed in the Patent Office the inventor was presumed to have disclosed an invention which, but for the delays inherent in prosecution, would have been disclosed to the public on the filing date.” *In re Wertheim*, 646 F.2d 527, 536 (CCPA 1981); *see also id.* at 532 (discussing *Alexander Milburn Co. v. Davis-Bourbonville Co.*, 270 U.S. 390 (1926), and that § 102(e) is “a codification of the rule of” the *Milburn* case).

Therefore, under the reasoning of these cases, a patent may be considered prior art as of the date of a provisional application so long as the provisional disclosed (sufficiently under § 112) the same invention eventually claimed in the patent. As a result, if the patent is shown to have at least one claim to an invention that is supported by the disclosure of a provisional application, it can be said that the provisional disclosed the same invention eventually claimed in the patent, and the patent may be considered prior art as of the filing date of the provisional under § 102(e)(2).

Here, Petitioner asserts that the Portnoy patent is entitled to a priority date “as of January 29, 2002 (the filing date of the later filed ’894 Provisional Application).” Pet. 10; *see also id.* at 9 (“Portnoy is [p]rior [a]rt [a]t [l]east [a]s [o]f January 29, 2002.” (emphasis omitted)). According to Petitioner, “both the [Portnoy] ’894 Provisional and the [Portnoy] ’196 Provisional supports claim 1 of Portnoy.” Pet. 15 (citing Ex. 1002 ¶ 95). To

IPR2020-00879

Patent 7,260,846 B2

support its position, Petitioner provides a claim chart identifying written description in *both* of the Portnoy Provisional Applications for every limitation in Claim 1 of the Portnoy patent (Ex. 1004). Pet. 11–14 (citing Exs. 1002, 1005, 1007); *see Dynamic Drinkware*, 800 F.3d at 1381–82. And in its analysis of the challenged claims of the '846 patent, Petitioner provides parallel citations to the Portnoy patent and the corresponding disclosures in Portnoy's provisional applications (*see generally* Pet. 30–70; *see also* Ex. 1002, 41–101) to demonstrate that the relevant disclosures of the Portnoy patent were carried over from the Portnoy Provisional Applications. *See In re Giacomini*, 612 F.3d 1380, 1383 (Fed. Cir. 2010) (holding that a claim is unpatentable “if another’s patent discloses the same invention, which was carried forward from an earlier U.S. provisional application or U.S. non-provisional application”).

In response, Patent Owner maintains that the Portnoy patent does not qualify as prior art “[b]ecause the Portnoy '196 Provisional Application and the Portnoy '894 Provisional Application both fail the disclosure requirement and claims requirement set forth by *Dynamic Drinkware*.” PO Resp. 13. More particularly, Patent Owner argues that: (i) neither the Portnoy '196 Provisional Application nor the '894 Provisional Application provides sufficient § 112 support for a “computer system,” as set forth in the preamble of claim 1 of the Portnoy patent (PO Resp. 14; Sur-Reply 10); (ii) claim 1 of the '966 Patent is directed to ineligible subject matter under 35 U.S.C § 101, and as such, it is not a claimed invention and cannot be relied on as prior art (PO Resp. 15–17; Sur-Reply 11); and (iii) “the disclosures of [the Portnoy patent] that Petitioner identifies as allegedly providing support for its obviousness analysis are not adequately supported

in the provisional applications” (PO Resp. 17–22; Sur-Reply 5–6). We address each argument in turn.

*a. Whether the Portnoy Provisional Applications support a “computer system”*

Patent Owner asserts that claim 1 of the Portnoy patent “requires a ‘computer system,’” but neither the Portnoy ’196 Provisional Application nor the ’894 Provisional Application “represents a ‘computer system’ as described in the [S]pecification as well as the only independent claim (claim 1) of the Portnoy ’966 Patent.” PO Resp. 14; Sur-Reply 3–4. Patent Owner acknowledges that “the Portnoy ’196 and ’894 Provisionals may mention an ‘intrusion detection system’ (IDS),” but argues that neither provisional application “disclose[s] an IDS system.” PO Resp. 14 (citing Ex. 1007, 1).

Having considered the arguments and evidence presented during trial, we determine that Petitioner persuasively shows that the Portnoy Provisional Applications provide adequate support for using a “computer system” as set forth in the preamble of claim 1 of the Portnoy patent. Ex. 1004, 29:27–28 (The preamble of claim 1 sets forth “[a] method for unsupervised detection of an anomaly in the operation of a computer system.”).

To satisfy the written description requirement, the claimed subject matter need not be described *“in haec verba”* in the original disclosure. *See In re Wright*, 866 F.2d 422, 425 (Fed. Cir. 1989). Rather, the test for determining compliance with the written description requirement is whether the original disclosure of the patent application reasonably conveys to a person of ordinary skill in the art that the inventor had possession of the claimed subject matter as of the filing date. *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (en banc).

The Portnoy '894 Provisional<sup>10</sup> is titled “A Geometric Framework for Unsupervised Anomaly Detection: Detecting Intrusions in Unlabeled Data.” Ex. 1007, 1. The '894 Provisional discloses, by way of introduction, that “[i]ntrusion detection systems (IDSs) are an integral part of any complete security package of a modern, well managed network system.” *Id.* The Portnoy '894 Provisional describes “a new geometric framework for *unsupervised anomaly detection*, which are algorithms that are designed to process unlabeled data.” *Id.* The Portnoy '894 Provisional presents a framework in which “data elements are mapped to a feature space” and discloses “three algorithms for detecting which points lie in sparse regions of the feature space.” *Id.* The Portnoy '894 Provisional further describes evaluating its approach “by performing experiments over network records from the KDD CUP 1999 data set and system call traces from the 1999 Lincoln Labs DARPA evaluation.” *Id.*

Patent Owner argues that “[t]he Portnoy Provisionals do not disclose a computer system within the scope of [c]laim 1 in part because the Portnoy Provisionals do not disclose a working IDS.” Sur-Reply 3. According to Patent Owner,

[a] POSITA would understand, at the very least, that an IDS system operates inside a computer system and contains the ability to extract and analyze data. Ex. 2001, ¶ 57. Although the algorithms disclosed may correspond to those that can be programmed into a computer, a working computer system would collect and store data in order to perform operations on that data to reach a conclusion. *Id.* These steps are not disclosed by the Portnoy '196 and '894 Provisionals.

---

<sup>10</sup> Petitioner asserts that the Portnoy patent is entitled to a priority date “as of January 29, 2002 (the filing date of the later filed '894 Provisional Application).” Pet. 10.

PO Resp. 14. However, we agree with Petitioner “that Portnoy’s provisional applications need not disclose a specific type or design of a computer system.” Pet. Reply 4. Instead, the Portnoy Provisional Applications need only reasonably convey to a person of ordinary skill in the art that the inventor had possession of the claimed subject matter as of the filing date. *Id.*; *Ariad*, 598 F.3d at 1351. And, to the extent Patent Owner asserts that the Portnoy Provisional Applications fail to convey adequately to one of ordinary skill in the art that the inventor had possession of the steps of “collect[ing] and stor[ing] data,” Patent Owner’s argument is unpersuasive, at least because claim 1 of the Portnoy patent does not recite such subject matter. *See* Ex. 1004, 29:27–28; *Cf.* Pet. 11–14; *see also Dynamic Drinkware*, 800 F.3d at 1382 (“A provisional application’s effectiveness as prior art depends on its written description support for the claims of the issued patent of which it was a provisional.”).

Patent Owner directs attention to the deposition testimony of Dr. Srivastava during cross examination. *Id.* at 3–4. According to Patent Owner,

Petitioner’s expert testified that the Portnoy Provisionals do not disclose an “operational system.” (“Q: What do you mean by real world system? A: Operational system. One that is in this particular context one that is actually operationally deployed. Q: So, Portnoy does not expressly disclose an operation[al] system, right? A: At least not in exhibits 1005 and 1007 that we just discussed.”).

Sur-Reply 3 (citing Ex. 2003, 148:13–21). Based on this testimony, and relying on its expert witness, Mr. Jawadi, Patent Owner concludes that “the Portnoy Provisionals do not disclose the required computer system.” *Id.* at 4 (citing Ex. 2001 ¶¶ 45–47, 50, 57).

However, we do not understand the relied upon portion of Dr. Srivastava's deposition testimony to support Patent Owner's contention that the Portnoy Provisionals fail to provide adequate disclosure for the "computer system" in claim 1 of the Portnoy patent. In our opinion, Dr. Srivastava's testimony simply provides us with the understanding that the Intrusion Detection System (IDS), disclosed in conjunction with the "geometric framework for unsupervised anomaly detection," in the Portnoy Provisional Applications, was not "operationally deployed." Ex. 2003, 148:15–21. We find Dr. Srivastava's deposition testimony to be consistent with what Dr. Srivastava opined in his declaration testimony, i.e., "Portnoy is a proof of concept for a live system." Ex. 1002 ¶ 122; *see also id.* ¶ 128 ("Portnoy is a test of a live system relying on a prebuilt dataset.").

To the extent that Patent Owner relies upon the deposition testimony from Mr. Jawadi to contradict Dr. Srivastava's deposition testimony (Sur-Reply 4 (citing Ex. 2001 ¶¶ 45–47, 50, 57)), we find such reliance to be unpersuasive at least because Mr. Jawadi simply parrots Patent Owner's argument and provides little if any analysis in support. Instead, we credit, and give greater weight, to Dr. Srivastava's deposition testimony that one of ordinary skill in the art

would have understood that the '894 Provisional Application discloses *[a] method for unsupervised detection of an anomaly in the operation of a computer system comprising*, as claim 1's preamble recites. The entirety of the '894 Provisional Application is directed to a geometric framework for unsupervised anomaly detection, which is *[a] method for unsupervised detection of an anomaly*. *See e.g.*, Ex. 1007 at p. 1 (Title) and (Abstract). Given that the paper explains its methodology in the context of intrusion detection systems, a POSITA in the art would have understood that the '894 Provisional Application is aimed at detecting anomalies in *the*

*operation of a computer system.* Similarly, the '196 Provisional also “present[s] a new type of clustering-based intrusion detection algorithm, *unsupervised anomaly detection.*” Ex. 1005 at p. 1 (Abstract) (emphasis in the original).

Ex. 1002 ¶ 90; *see also* Pet. Reply 2 (citing Ex. 1002 ¶ 90 (“[A] POSITA would have understood that the provisional applications disclose “detecting anomalies in *the operation of a computer system.*”)). Thus, we determine that Petitioner has sufficiently shown that the Portnoy Provisional Applications provide adequate support for using a “computer system.”

*b. Whether claim 1 of the '966 Patent is directed to ineligible subject matter under 35 U.S.C § 101 rendering it unavailable as prior art?*

Patent Owner asserts that the Portnoy patent cannot claim priority to the Portnoy Provisional Applications because “[c]laim 1 of Portnoy is directed to nothing more than an abstract idea, and is not patentable.” PO Resp. 15–16. According to Patent Owner, “[t]he claims of the alleged reference must be directed to inventive subject matter in order to provide support for an analysis under *Dynamic Drinkware.*” Sur-Reply 11.

In response, Petitioner argues that “there is no known precedent requiring consideration of patent subject matter eligibility for determining prior art eligibility.” Pet. Reply 15. Petitioner explains

35 U.S.C. § 102(e) expressly applies to both “an application for patent” and “a patent granted on an application for patent.” *See* 35 U.S.C. § 102(e). The statue’s applicability to both patent applications and patents demonstrates that patent eligibility [is] immaterial to whether a reference can serve as prior art because patent applications often contain unexamined claims. Indeed, even abandoned applications may serve as prior art under 35 U.S.C. § 102(e) regardless of the reason for their abandonment, which may include failure to recite eligible subject matter. *See* MPEP [§] 901.02. Thus, there is no requirement that a claim

recite patent eligible subject matter for a reference to qualify as prior art under 35 U.S.C. § 102(e).

*Id.* We agree with Petitioner.

The Federal Circuit has explained the conditions under which an issued patent is entitled to the filing date of a provisional application for prior art purposes, stating

for a non-provisional application to claim priority to a provisional application for prior art purposes, “the specification of the provisional [application] must contain a written description of the invention . . . in such full, clear, concise, and exact terms, to enable an ordinarily skilled artisan to practice the invention claimed in the non-provisional application.” Further, we have previously stated that “for the non-provisional utility application to be afforded the priority date of the provisional application . . . the written description of the provisional must adequately support the claims of the non-provisional application.”

*Amgen Inc. v. Sanofi*, 872 F.3d 1367, 1380 (Fed. Cir. 2017) (quoting *Dynamic Drinkware*, 800 F.3d at 1378 and *New Railhead*, 298 F.3d at 1294, (alterations in original)). Thus, our reviewing court has determined that entitlement to a claim of priority is based on whether the written description of the provisional application adequately supports the claims. Here, Patent Owner identifies no authority, nor are we aware of any such authority, holding that the claims of an alleged prior art reference must be directed to patent-eligible subject matter for an analysis under *Dynamic Drinkware*. Sur-Reply 11. Accordingly, we agree with Petitioner that it may rely on the Portnoy patent as prior art under the circumstances presented.

- c. Whether the portions of the Portnoy patent that Petitioner identifies as allegedly providing support for its obviousness analysis are adequately supported in the Portnoy Provisional Applications?*

Patent Owner asserts that the Portnoy Provisional Applications do not disclose the “monitoring,” “extracting,” and “storing” limitations recited by challenged claim 7. PO Resp. 17–22; Sur-Reply 5–6. And, “[b]ecause Petitioner has not shown ‘the subject matter relied upon in the [Portnoy] patent is described in the provisional application[s]’ the analysis fails the *Drinkware* test.” PO Resp. 22. We disagree.

At the outset, we note that Petitioner relies on the Portnoy Provisional Applications in an obviousness challenge. We address whether the Portnoy Provisional Applications teach or disclose certain limitations of challenged claim 7, such as “monitoring,” “extracting,” and “storing,” further below. However, in order to determine if Petitioner meets its burden of showing that the Portnoy patent properly claims priority to the Portnoy Provisional Applications under *Dynamic Drinkware*, the proper comparison is between the claims of the Portnoy patent (not the claims of the ’846 patent) and the Portnoy Provisional Applications. Pet. Reply 5–6. As discussed above, Petitioner provides a claim chart identifying written description in *both* of the Portnoy provisional applications for every limitation in claim 1 of the Portnoy patent. Pet. 11–14.

Accordingly, we are persuaded that Petitioner has met its burden of showing, by a preponderance of the evidence, that the Portnoy patent properly claims priority to the Portnoy ’196 Provisional Application and the Portnoy ’894 Provisional Application. Therefore, we determine that the Portnoy patent is available as a prior art reference with an effective date of the filing date of at least the later filed Portnoy ’894 Provisional Application for subject matter carried over to the Portnoy patent from the Portnoy Provisional Applications.

*d. Conclusion*

Upon review of the Petition and the full trial record, we are persuaded that Petitioner has met its burden of showing, by a preponderance of the evidence, that the Portnoy patent is prior art to the '846 patent.

Having determined that the Portnoy patent is prior art under 35 U.S.C. § 102(e), we discuss the remaining references asserted in Ground 1.

*3. Overview of Cannady (Ex. 1012)*

Cannady is a journal article titled “Artificial Neural Networks for Misuse Detection.” Ex. 1012, 1. Cannady presents an analysis of the applicability of neural networks in the identification of instances of external attacks against a network ranging from denial of service attacks to port scans. *Id.* at 1, 7. Cannady explains that an artificial neural network consists of a collection of processing elements that are highly interconnected and transform a set of inputs to a set of desired outputs. *Id.* at 3. A neural network conducts an analysis and provides a probability estimate that the data matches the characteristics which it has been trained to recognize. *Id.*

The neural network gains experience initially by training the system to correctly identify preselected examples of the problem. Ex. 1012, 4. The response of the neural network is reviewed and the configuration of the system is refined until the neural network’s analysis of the training data reaches a satisfactory level. *Id.* In addition to the initial training period, the neural network also gains experience over time as it conducts analyses on data related to the problem. *Id.* The constantly changing nature of network attacks requires a flexible defensive system that is capable of analyzing the enormous amount of network traffic in a manner which is less structured than rule-based systems. *Id.*

According to Cannady, a neural network-based misuse detection system could potentially address many of the problems that are found in rule-based systems. *Id.* Cannady describes various advantages of utilizing a neural network in the detection of instances of misuse, including: flexibility, non-linear analysis, speed, and the ability of the neural network to gain experience and improve its ability to determine attacks. *Id.* at 5. Cannady discloses that the most important advantage of neural networks in misuse detection is the ability of the neural network to “learn” the characteristics of misuse attacks and identify instances that are unlike any which have been observed before by the network. *Id.*

Cannady describes two general implementations of neural networks in misuse detection systems: (1) incorporating them into existing or modified expert systems, and (2) involving the neural network as a standalone misuse detection system. *Id.* at 6. Cannady describes a prototype neural network that was designed to test the ability of a neural network to identify indications of misuse. *Id.* at 7. Data for training and testing the prototype was generated using the RealSecure™ network monitor.<sup>11</sup> *Id.* RealSecure™ is designed to be used by network security administrators to passively collect data from the network and identify indications of attacks. *Id.* In addition to the “normal” network activity that was collected as events by RealSecure™, the host for the monitor was “attacked” using the Internet Scanner™.<sup>12</sup> *Id.* Approximately 10000 individual events were collected by RealSecure™ and stored in a Microsoft Access™ database, of which approximately 3000 were

---

<sup>11</sup> The RealSecure™ network monitor is available from Internet Security Systems, Inc. Ex. 1012, 7.

<sup>12</sup> The Internet Scanner™ is available from ISS, Inc., and the Satan scanner. Ex, 1012, 7.

IPR2020-00879

Patent 7,260,846 B2

simulated attacks. *Id.* According to Cannady, the results of the testing demonstrate the potential of a neural network to detect individual instances of possible misuse from a representative network data stream. *Id.* at 9.

#### 4. *Overview of Barbara (Ex. 1013)*

Barbara is a journal article titled “Detecting Novel Network Intrusions Using Bayes Estimators.” Ex. 1013, 1. Barbara describes a pseudo-Bayes estimators technique to enhance an anomaly detection system’s ability to detect new attacks while reducing the false alarm rate as much as possible. *Id.* at 2. Barbara’s method is based on an anomaly detection system called Audit Data Analysis and Mining (ADAM). *Id.* ADAM applies mining association rules techniques to look for the abnormal events in network traffic data, then it uses a classification algorithm to classify the abnormal events into normal instances and abnormal instances. *Id.* The abnormal instances can be further categorized into attack names if ADAM has gained knowledge about the attacks. *Id.*

With the help of the classifier, the number of false alarms is greatly reduced because the abnormal associations that belong to normal instances will be filtered out. Ex. 1013, 2. Barbara explains that the normal instances and attacks that the classifier is able to recognize are limited to those that appear in the training data. *Id.* To overcome this limitation, Barbara describes applying the pseudo-Bayes estimators method as a means to estimate the prior and posterior probabilities of new attacks. *Id.* The method constructs a Naive Bayes classifier to classify the instances into normal instances, known attacks and new attacks. *Id.* According to Barbara, one advantage of pseudo-Bayes estimators is that no knowledge about new attacks is needed since the estimated prior and posterior

probabilities of new attacks are derived from the information of normal instances and known attacks. *Id.*

### 5. *Analysis of Claim 7*

Petitioner asserts claim 7 would have been obvious over Portnoy, Cannady, and Barbara. Pet. 30–60; Pet. Reply 16–26. Patent Owner contends that Petitioner has failed to establish that limitations [7.A], [7.B], and [7.C] are taught by the references. PO Resp. 25–32; Sur-Reply 5–8. Patent Owner further contends that there is no motivation to combine Barbara and Portnoy. PO Resp. 22–25; Sur-Reply 8–9.

Petitioner’s contentions regarding the preamble and limitations [7.D], [7.E], and [7.F] are undisputed.

We have reviewed the evidence and arguments provided by the parties and are persuaded that Petitioner has demonstrated by a preponderance of the evidence that claim 7 is unpatentable as obvious over Portnoy, Cannady, and Barbara.

We use Petitioner’s notations to identify the claim elements.

*a) “An intrusion detection method comprising the steps of:”*

Petitioner asserts that, to the extent the preamble is limiting, Portnoy discloses this limitation. Pet. 30 (citing Ex. 1004, code (54), 1:52–64, 4:31–34; Ex. 1005, Title, Abstract). We find that Petitioner’s contentions, which Patent Owner does not dispute, are persuasive in demonstrating that Portnoy discloses the preamble to the extent it is limiting.

*b) “Element [7.A]: monitoring network traffic passing across a network communications path”*

Petitioner contends that “Portnoy discloses, or at least renders obvious, this limitation alone or in view of Cannady and/or Barbara.” Pet. 30. For example, Petitioner asserts that “Portnoy discloses monitoring

network packets and connections passing across a network communications path in order to build the dataset.” Pet. 31 (citing Ex. 1005, 12; Ex. 1004, 8:21–25; Ex. 1002 ¶¶ 121, 126–128) (emphases omitted). Petitioner further asserts that Portnoy describes “how to implement a live system,” and explains, “that in practice, this would mean collecting raw data from the network, extracting feature values from it, and training on the resulting set of feature vectors.” Pet. 32 (citing Ex. 1005, 12; Ex. 1004, 8:21–25). According to Petitioner, “a POSITA would have understood that collecting data includes the act of monitoring data from the network traffic” (Ex. 1002 ¶ 126) and that “you cannot collect raw data in the manner Portnoy teaches without monitoring.” Pet. 32.

In response, Patent Owner contends “the Portnoy Provisional Applications do not disclose a system for the collection of data from an audit stream” (*id.* at ¶ 20 (citing Ex. 2001 ¶ 69)), and as such, neither the Portnoy patent nor the Portnoy Provisional Applications discloses “monitoring network traffic passing across a network communications path,” as recited by claim 7. PO Resp. 19, 26–30. However, based on the parties’ arguments and the complete record after trial, we agree with Petitioner that “Portnoy discloses monitoring network packets and connections passing across a network communications path in order to build the dataset.” Pet. 31 (citing Ex. 1005, 12; Ex. 1004, 8:21–25; Ex. 1002 ¶¶ 121, 126–128) (emphases omitted).

In this regard, Portnoy describes gathering raw network data during simulated intrusions and extracting feature values from the connection records. Ex. 1004, 20:17–23. Portnoy explains that “[a] connection is a sequence of TCP packets to and from some IP addresses” and “[t]he TCP packets were assembled into connection records.” *Id.* at 20:23–26. The

IPR2020-00879

Patent 7,260,846 B2

Petition relies on disclosure in the Portnoy '196 Provisional of “periodically (every 2 weeks for example) collecting raw data from the network” to support the above disclosure in Portnoy. Ex. 1005, 12. Portnoy also discloses that “[t]he network connection records used were the KDD Cup 1999 Data,” “which contained a wide variety of intrusions simulated in a military network environment.” Ex. 1004, 20:17–19; *see also* Ex. 1005, 4 (“The dataset used was the KDD Cup 1999 Data” which “contained a wide variety of intrusions simulated in a military network environment.”) (footnote omitted). It is apparent from this disclosure of Portnoy that the data gathered during the simulated intrusions includes network connection records based on TCP packets. Ex. 1004, 20:17–36.

Patent Owner argues that

nothing in [the Portnoy '196 Provisional Application] at p. 12 discloses a system for monitoring network packets or connections. Furthermore, Portnoy '196 Provisional, Ex. 1005, does not describe [a] network communications path. The Portnoy '196 Provisional, Ex. 1005, does not mention the terms monitor, sniff, communication, or path (in any conjugation).

PO Resp. 19 (citing Ex. 2001 ¶ 67). According to Patent Owner, “[t]here was no collection of raw data from a network in” the Portnoy '196 Provisional Application because “[t]he KDD CUP dataset was used” and “[w]hen this did not work, the KDD CUP dataset was modified by Portnoy to reduce the number of attacks that were represented. No POSITA would consider this to be ‘collected’ or ‘raw data.’” *Id.* at 20 (citing Ex. 2001 ¶ 69); *see also id.* at 29 (citing Ex. 2001 ¶ 92) (“[A] POSITA would understand that one can download the KDD CUP dataset and perform data analysis on it without it ever being ‘monitored.’”).

However, as Petitioner correctly notes, the cited portions of the Portnoy Provisional Applications do not simply refer to the KDD 1999 Cup dataset, but the cited portions also contemplate live implementation. *See* Pet. Reply 8–9 (citing Pet. 32, 37; Ex. 1002 ¶¶ 126–158, 148) (“Portnoy’s description of a live implementation demonstrates how a prebuilt dataset, like KDD Cup 1999 Dataset, would be built.”). For example, the Portnoy ’196 Provisional Application discloses that “[i]n practice, this would mean periodically (every 2 weeks for example) collecting raw data from the network, extracting feature values from it, and training on the resulting set of feature vectors.” Ex. 1005, 12. The Portnoy ’894 Provisional Application further discloses “[o]ur data is collected from some audit stream of the system.” Ex. 1007, 5; *see also id.* (“The key to our framework is mapping the records from the audit stream to a feature space.”). In light of these disclosures, we credit Dr. Srivastava’s declaration testimony that one of ordinary skill in the art

would have understood that collecting data includes the act of monitoring data from the audit streams or the network as a whole because in my experience and in the context of the ’894 Provisional Application, audit streams are streams of audit data from the network. In fact, Portnoy shares my understanding. Ex. 1004 at 8:21–25 (“one such concrete example of an audit stream may be network packet header data (without the data payload of the network packets) that are ‘sniffed’ at an audit point in the network.”). To have streams we must, in my experience, observe (“monitor”) the network traffic.

Ex. 1002 ¶ 126. To the extent Patent Owner relies on paragraphs 67 and 69 of Mr. Jawadi’s declaration testimony to rebut Dr. Srivastava’s testimony, Mr. Jawadi’s testimony merely repeats the Response’s assertions word-for-word and, thus, is not supported sufficiently by objective evidence or analysis. For this reason, we do not credit the testimony of Mr. Jawadi on

this issue. *See* 37 C.F.R. § 42.65(a) (“Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.”).

Patent Owner further asserts without any explanation that “Petitioner has not shown how experimenting on simulated data meets the limitation for ‘monitoring network traffic.’” PO Resp. 28 (citing Ex. 2001 ¶ 90). However, as Petitioner points out, “[i]n describing how to implement a live system, Portnoy states that in practice, this would mean collecting raw data from the network, extracting feature values from it, and training on the resulting set of feature vectors.” Pet. 32 (citing Ex. 1005, 12; Ex. 1004, 8:21–25). And, as we stated in the Decision on Institution, “[w]e see nothing in claim 7 that excludes network traffic that includes *simulated* intrusions. In other words, nothing in claim 7 includes a *bona fide* network attack or intrusion by some malicious entity.” Dec. on Inst. 36.

Patent Owner also directs attention to the deposition testimony of Dr. Srivastava. PO Resp. 27; Sur-Reply 5. According to Patent Owner, “Portnoy does not disclose monitoring network traffic passing across a network communications path” because Dr. Srivastava admitted “that the Portnoy ’196 Provisional and the Portnoy ’894 Provisional do not contain ‘any sort of monitoring tool.’” PO Resp. 27 (citing Ex. 2003, 147:11–15). However, as Petitioner correctly points out, claim 7 does not recite a “monitoring tool.” Here, we credit, and give greater weight to Dr. Srivastava’s declaration testimony that one of ordinary skill in the art “would have understood that you cannot collect raw data in the manner Portnoy teaches without monitoring because in my experience, monitoring network traffic is one of the first steps in collecting information from a network.” Ex. 1002 ¶ 127. With this understanding, we agree with

Petitioner that one of ordinary skill in the art “reading Portnoy would find this element obvious at least because Portnoy discloses how the underlying dataset was created and that for a live system “this would mean . . . collecting raw data from the network.” Pet. Reply 20 (citing Ex. 1005 4, 12; Pet. 32; Ex. 1002 ¶¶ 126–131). Thus, we find that Petitioner has provided persuasive evidence that both Portnoy and the Portnoy Provisional Applications disclose “monitoring network traffic passing across a network communications path,” as required by claim 7, for the reasons set forth in the Petition. Pet. 31 (citing Ex. 1005, 12; Ex. 1004, 8:21–25; Ex. 1002 ¶¶ 121, 126–128) (emphases omitted).

Even if Portnoy does not explicitly disclose “monitoring network traffic passing across a network communications path,” as recited by element [7.A], Petitioner contends that “it would have been obvious to a POSITA to *monitor*, as taught by Cannady, the TCP packets (*network traffic*) *passing across* the connection to and from IP addresses or the connection in a military network environment (*network communications path*) of Portnoy.” Pet. 32 (citing Ex. 1012). Petitioner asserts that “Cannady discloses that intrusion detecting includes ‘receiv[ing] data from the network stream and analyz[ing] the information for instances of misuse.’” *Id.* (citing Ex. 1012, 6) (emphasis omitted). Petitioner explains that Cannady discloses a network packet monitoring tool, i.e., “RealSecure™ monitor,” that is configured to “capture the data for each event which would be consistent with a network frame” and is designed “to passively collect data from the network.” *Id.* at 32–33 (citing Ex. 1012, 7 (emphasis omitted); Ex. 1002 ¶¶ 132–133). Petitioner provides several reasons why one of ordinary skill in the art would have turned to the analogous art of Cannady “to apply the well-known teaching of *monitoring*

to Portnoy's *network traffic passing across a network communications path.*" *Id.* at 34–36 (citing Ex. 1002 ¶¶ 126–128, 137, 139–145; Ex. 1012, 1, 7, 9–12; Ex. 1013, 1–4, 11–15).

In response, Patent Owner argues that one of ordinary skill in the art would not have considered Cannady to have disclosed "monitoring network traffic passing across a communication path" because "Cannady openly admits to not having a working system." PO Resp. 26 (citing Ex. 2001 ¶ 81); Sur-Reply 6–7 (citing Ex. 2001 ¶ 83). According to Patent Owner, Petitioner overlooks the "Future Work" section of the Cannady paper, which states that "[a] complete system will require the ability to directly receive inputs from a network data stream. The most difficult component of the analysis of network traffic by a neural network is the ability to effectively analyze the information in the data portion of an IP datagram. The various commands that are included in the data often provide the most critical element in the process of determining if an attack is occurring against a network."

PO Resp. 26 (quoting Ex. 1012, 11); Ex. 2001 ¶ 81. Patent Owner's argument does not undermine Petitioner's showing.

Patent Owner's assertion that Cannady cannot teach "monitoring network traffic passing across a communication path" because of the difficulties related to the "analysis of network traffic by a neural network" (PO Resp. 26), fails to address Petitioner's primary argument, i.e., that Cannady teaches the use of commercially available monitoring tool to monitor network traffic, as claim 7 requires. Pet. 32–33 (citing Ex. 1012, 6, 7; Ex. 1002 ¶¶ 132–133). Rather than address Petitioner's argument and evidence, Patent Owner, relying on its expert, Mr. Jawadi, asserts that one of ordinary skill in the art would not have "consider[ed] Cannady to have disclosed 'monitoring network traffic passing across a communication

IPR2020-00879

Patent 7,260,846 B2

path.’’ Sur-Reply 7 (citing Ex. 2001 ¶ 83). According to Mr. Jawadi, ‘‘Cannady indicates that Cannady does not describe a complete system’’ and ‘‘does not suggest that using RealSecure would be viable [in a neural network], because Cannady requires the ability to ‘directly receive inputs.’’’ Ex. 2001 ¶ 83 (citing Ex. 1012, 11).

However, as Petitioner correctly notes, it is unclear how any difficulties with neural networks or Cannady’s discussion about its ‘‘Future Work’’ otherwise negates its teachings regarding ‘‘RealSecure™ monitor.’’ *See* Ex. 1012, 7 (‘‘RealSecure™ is designed to be used by network security administrators to passively collect data from the network and identify indications of attacks.’’). We credit Dr. Srivastava’s declaration testimony that ‘‘Cannady’s RealSecure™ is just one example of well-known and commercially available tools for monitoring network traffic.’’ Ex. 1002 ¶ 133. Thus, we agree with Petitioner and Dr. Srivastava that one of ordinary skill in the art would have understood that applying Cannady’s ‘‘known techniques to Portnoy’s known system would achieve the predictable result of a real-world version of Portnoy that monitors network traffic.’’ Pet. 35 (citing Ex. 1002 ¶¶ 139–145).

Even if Portnoy and Cannady do not explicitly disclose the argued limitation, Petitioner contends that Barbara separately discloses monitoring network traffic. Pet. 33 (citing Ex. 1013, 2). According to Petitioner, Barbara discloses that its ‘‘preprocessing engine sniffs TCP/IP traffic data, and extracts information from the header of each connection.’’ *Id.* (quoting Ex. 1013, 2); Ex. 1002 ¶ 134.

Based on the above, Petitioner concludes that

Portnoy alone, or in combination with Cannady or Barbara, discloses, or renders obvious, Element [7.A]. Ex. 1002 at

¶¶135–136. Specifically, Portnoy combined with Cannady would result in Portnoy’s intrusion detection system that monitors network traffic using Cannady’s teachings of the RealSecure™ monitor, or similar tools. Ex. 1002 at ¶¶139–140. Also, Portnoy combined with Barbara would result in an intrusion detection system (“IDS”) incorporating the teachings of preprocessing module that sniffs TCP/IP traffic. *Id.*

Pet. 33–34. Petitioner provides several reasons why one of ordinary skill in the art would have turned to the analogous art of Barbara “to apply the well-known teaching of *monitoring* to Portnoy’s *network traffic passing across a network communications path.*” *Id.* at 34–36 (citing Ex. 1002 ¶¶ 126–128, 137, 139–145; Ex. 1012, 1, 7, 9–12; Ex. 1013, 1–4, 11–15).

Patent Owner does not dispute Petitioner’s contentions regarding Barbara with respect to this limitation. PO Resp. 30. Instead, Patent Owner’s argument is that “there is no motivation to combine Portnoy with Barbara.” *Id.*; Sur-Reply 8–9.

Patent Owner asserts that Portnoy is directed to unsupervised anomaly detection which “does not require a purely normal training set” and can detect anomalies over unlabeled or raw data. PO Resp. 22–24; Sur-Reply 8–9. However, in contrast, Patent Owner contends that Barbara’s anomaly detection system detects new attacks using a supervised anomaly detection method which requires a large training set. PO Resp. 24–25; Sur-Reply 8–9. According to Patent Owner,

[b]ecause the system disclosed in Portnoy’s patent sets out to detect anomalies in an unsupervised environment with a small training set, and because Barbara attempts to detect anomalies in a supervised setting, with a large training set, there would be no motivation to combine. Ex. 2001, ¶ 81. For example, Barbara requires the labeling of data, and a data mining period with no attacks. *Id.* After the data is mined, Barbara analyzes the data using a probabilistic approach. *Id.* A POSITA would view these

are two very different approaches to anomaly detection, and would not choose to combine them. *Id.*

PO Resp. 25; Sur-Reply 8.

Petitioner responds that “[w]hether Barbara and Portnoy use different anomaly detection approaches is irrelevant.” Pet. Reply 16. Petitioner adds that it “does not rely on Barbara to ‘identify anomalous behavior,’” as limitation [7.E] recites.<sup>13</sup> Pet. Reply 16 (citing Pet. 49–52). Relying on the declaration testimony of its expert, Dr. Srivastava, Petitioner asserts that one of ordinary skill in the art “would turn to Barbara for pre and post anomaly detection activity that “merely tak[e] the next logical step from proof of concept to live system” or “further refine Portnoy’s system and reduce false positives.” *Id.* (citing Ex. 1002 ¶ 139, 168, 174, 236, 241–242; Pet. 34–35, 39–41, 55.57).

Petitioner explains that “Barbara details of how to ‘monitor[]’ and ‘extract[]’ information used by Portnoy’s anomaly detection, and how to ‘classify[]’ an anomaly after it has been detected.” *Id.* at 16–17 (citing Pet. 32–36, 37–41, 53–57). And, according to Petitioner, “Patent Owner does not dispute that Barbara teaches these elements and provides no reason why using a different form of anomaly detection would impact pre or post anomaly detection processes.” *Id.*

In response, Patent Owner asserts that the statements made by “Petitioner are incorrect.” Sur-Reply 8. Relying on its expert, Mr. Jawadi, Patent Owner concludes that because Portnoy is directed to an unsupervised system and Barbara is directed to a supervised system, one of ordinary skill

---

<sup>13</sup> As discussed below in Section III.D.5.F, Petitioner asserts that “Portnoy discloses, or at least renders obvious, Element [7.E].” Pet. 49–52. Patent Owner does not dispute Petitioner’s contentions regarding limitation [7.E].

in the art “would view these as two very different approaches to anomaly detection and would not choose to combine them.” *Id.* (citing Ex. 2001 ¶ 80).

We have considered Patent Owner’s arguments, but they do not undermine Petitioner’s showing. Although Mr. Jawadi testifies in support of Patent Owner’s position, we find the testimony of Dr. Srivastava more credible on this issue. Ex. 1002 ¶ 139, 168, 174, 236, 241–247. Mr. Jawadi’s declaration merely parrots the Patent Owner Response without providing a persuasive explanation for the assertion that a person of ordinary skill in the art would not “choose to combine” Portnoy and Barbara. PO Resp. 25; Sur-Reply 8; *compare* Ex. 2001 ¶ 80. As Petitioner correctly notes, “Patent Owner does not dispute that Barbara’s approach to ‘monitoring’ and ‘extracting’ are examples of widely known techniques that any POSITA would have known.” Pet. Reply 17 (citing Pet. 32–41; Ex. 1002 ¶ 127–135, 139, 155–164). And, other than asserting that Barbara and Portnoy use different techniques for classification, Patent Owner does not identify any particular obstacle that a person of ordinary skill in the art would have understood to exist by using Barbara’s classifiers to process the output of Portnoy’s analysis. Pet. 55 (citing Ex. 1002 ¶¶ 230, 245–247).

For these reasons, we find and determine that Petitioner persuasively shows that “Portnoy discloses, or at least renders obvious, this limitation alone or in view of Cannady and/or Barbara.”

c) “Element [7.B]: extracting network packets from said passing traffic”

Petitioner contends that that “Portnoy alone, or in view of Cannady or Barbara, discloses, or at least renders obvious, Element [7.B].” Pet. 36. For example, Petitioner asserts

[a] POSITA would have understood that Portnoy’s proven algorithm teaches, or at least renders obvious, *extract[ion] of network packets* resulting in the prebuilt dataset because data, even if simulated, has to be acquired from somewhere in order to be analyzed. *See* Ex. 1002 at ¶146–155. At the very least, extraction of packets is a common, if not the most common, way of gathering such data. *See* Ex. 1002 at ¶163.

Pet. 36–37. Petitioner further asserts that Portnoy discloses “collect[ing] raw data from the network” (Pet. 37 (quoting Ex. 1005, 12)) and collecting data “from some audit stream” (Pet. 37 (quoting Ex. 1007, 5)), and as such, one of ordinary skill in the art “would have understood that collecting raw data and data from networks and audit streams, respectively, is, or at least renders obvious, *extracting network packets from said passing traffic.*” Pet. 37 (citing Ex. 1002 ¶ 148).

In response, Patent Owner contends that neither the Portnoy patent nor the Portnoy Provisional Applications discloses “extracting network packets,” as recited by claim 7. PO Resp. 17. Patent Owner argues that Petitioner improperly asserts that ““Portnoy operates by first extracting network traffic information”” when claim 7 requires “extracting network packets.” *Id.* (quoting Pet. 8 (citing Ex. 1005, 2, 4, 7; Ex. 1004, 8:21–34)). According to Patent Owner the Portnoy ’196 Provisional Application “only mentions extracting features, not extracting packets.” *Id.* at 18 (citing Ex. 2001 ¶ 59).

However, the Portnoy patent discloses that a connection record obtained from raw network data are “a sequence of TCP packets.” Ex. 1004, 20:23–24; *see also* Ex. 1005, 4 (“[a] connection is a sequence of TCP packets . . .”). We credit Dr. Srivastava’s statement that one of ordinary skill in the art

IPR2020-00879

Patent 7,260,846 B2

would have understood that Portnoy necessarily requires, or at least suggests, extracting network packets in order to build Portnoy's prebuilt dataset, or as Portnoy puts it, "feature vectors collected from the network." *See* Ex. 1005 at p. 12; Ex. 1004 at 20:21–23. Moreover, collecting data from audit streams is, or at least a POSITA [would] have understood that is, "extracting" as claimed. Ex. 1007 at p. 5; Ex. 1005 8:21–25.

Ex. 1002 ¶ 148. Patent Owner has not offered any persuasive argument or technical reasoning to explain how the claimed "extracting network packets from said passing traffic" is patentably distinguishable over the gathering of network data, including network packets (TCP packets), disclosed in both Portnoy and the Portnoy Provisional Applications.

Patent Owner's reliance on paragraph 59 of its expert, Mr. Jawadi's declaration testimony, does little to alter our conclusion. Here, Mr. Jawadi simply states

in my opinion, the Portnoy '894 Provisional, alone or in combination with the Portnoy '196 Provisional discussed above, does not contain a written description of the invention of the Portnoy '966 Patent in full, clear, concise, and exact terms to enable a POSITA to practice the inventions claimed in the Portnoy '966 Patent.

Ex. 2001 ¶ 59. Mr. Jawadi's declaration testimony is conclusory, is not supported sufficiently by any objective evidence or analysis and, thus, is entitled to little, if any, weight. *See* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight."). Thus, we find that Petitioner has provided sufficient evidence that both Portnoy and the Portnoy Provisional Applications disclose "extracting network packets from said passing traffic," as required by claim 7, for the reasons set forth in the Petition. Pet. 36–37 (citing Ex. 1005, 12; Ex. 1007, 5; Ex. 1004, 8:21–25; Ex. 1002 ¶¶ 146–155).

Even if Portnoy does not explicitly disclose “extracting network packets from said passing traffic,” Petitioner contends that “it would have been obvious to a POSITA to *extract*, as taught by Cannady, TCP packets (*network packets*) from the passing traffic of TCP packets flowing across the connection.” Pet. 37 (citing Ex. 1002 ¶¶ 154–155). Petitioner asserts that Cannady’s RealSecure™ monitor is configured to collect data from the network and “capture the data for each event which would be consistent with a network frame.” Pet. 37 (citing Ex. 1012, 7). Petitioner explains that one of ordinary skill in the art “would have understood that network frames correspond to network packets” (Pet. 38 (citing Ex. 1002 ¶ 157)), and “Cannady confirms this when disclosing the type of information RealSecure™ collects and how Cannady’s analysis uses such information.” Pet. 38 (citing Ex. 1012, 7–8; Ex. 1002 ¶¶ 157–159).

Petitioner also contends that “Barbara teaches, or renders obvious, “extracting network packets from said passing traffic,” as recited by element [7.B]. Pet. 38–39. For example, Petitioner asserts that Barbara discloses “‘look[ing] at TCP/IP traffic, and generat[ing] a record for each connection from the header information of its packets.’” Pet. 38 (quoting Ex. 1013, 4). According to Petitioner, “[a] POSITA would have understood that to ‘generate a record for each connection from the header information of its packets’ the packets are extracted.” Pet. 38 (citing Ex. 1002 ¶ 161).

Based on the above, Petitioner concludes that

Portnoy alone, or in combination with Cannady or Barbara, discloses, or render obvious Element [7.B]. Ex. 1002 at ¶¶ 165–175. Specifically, Portnoy combined with Cannady would result in an IDS that uses the teachings of well-known commercial tools to extract network packets. Ex. 1002 at ¶¶ 167–170. And Portnoy combined with Barbara would result in an IDS that uses

well-known packet sniffing techniques to extract network packets. *Id.*

Pet. 39. Petitioner provides several reasons why one of ordinary skill in the art “would have been motivated to combine the teachings of Cannady and/or Barbara” to Portnoy’s intrusion detection system. Pet. 39–41 (citing Ex. 1002 ¶¶ 147–150, 166–175; Ex. 1004, 8:21–25; Ex. 1005, 12; Ex. 1012, 7).

Patent Owner does not dispute Petitioner’s contentions regarding Cannady or Barbara with respect to this limitation. PO Resp. 30. Instead, Patent Owner asserts

Portnoy, Cannady and Barbara do not render obvious “monitoring a network communication path.” Portnoy and Cannady do not disclose monitoring network traffic passing across a communication path, and there is no motivation to combine Portnoy with Barbara. For the same reasons, there is no disclosure of “extracting network packets from said passing traffic.”

*Id.*

Patent Owner’s argument does not undermine Petitioner’s showing. For the reasons discussed above, and in Section III.D.5.A, Petitioner persuasively shows that “Portnoy alone, or in view of Cannady or Barbara, discloses, or at least renders obvious “extracting network packets from said passing traffic.”

*d) “Element [7.C]: storing individual components of said network packets in a database”*

Petitioner contends that “Portnoy, alone or in combination with Cannady, discloses, or at least renders obvious, Element [7.C].” Pet. 41. For example, Petitioner asserts that Portnoy’s disclosure of “extracted features” from TCP connections is equivalent to “individual components of said network packets.” Pet. 41 (citing Ex. 1005, 4; Ex. 1004, 20:44–58).

IPR2020-00879

Patent 7,260,846 B2

Petitioner further asserts that Portnoy discloses storing this information “in a database” as claimed because the KDD Cup 1999 Dataset is “a database.” Pet. 42 (citing Ex. 1005, 4; Ex. 1004, 20:18–58). According to Petitioner, one of ordinary skill in the art “would have understood that the information Portnoy uses is *individual components of network packets* because TCP connections are actually just network packets and exist within the data contained in the packets thus descriptions or data about TCP connections comes from data in the network packets.” Pet. 42 (citing Ex. 1002 ¶ 179).

In response, Patent Owner contends that

Petitioner does not point to a single disclosure of a database within any of the Portnoy references. Instead, Petitioner merely suggests that since the ’966 Patent refers to “extracted features” of a TCP Connection, that “a POSITA would have understood that Portnoy discloses, or at least suggests, storing individual components in its dataset.”

PO Resp. 30–31.

Patent Owner’s argument does not undermine Petitioner’s showing. Instead, we agree with Petitioner that the Portnoy Provisional Applications “disclose the KDD Cup 1999 Dataset, which is a database storing extracted features of network packets (i.e., central location to store data), and an example of the data that a live system would collect and store.” Pet. Reply 11 (citing Petition 42–43; Ex. 1002 ¶179–183). Petitioner’s position is supported by Dr. Srivastava’s opinion that one of ordinary skill in the art would

have understood that a live implementation of Portnoy would necessarily require, or at least it would have been obvious to a POSITA that Portnoy would need to carry out, “storing individual components of said network packets in a database” in order to store the same kind of information stored in the prebuilt

data set. Otherwise, Portnoy would not have the data needed to perform its analysis.

Ex. 1002 ¶ 181.

Patent Owner disagrees. Relying on the declaration testimony of Mr. Jawadi, Patent Owner asserts that “[t]he implementation of a database connected to a system which monitors a communication stream and extracts data would not have been an [sic] obvious, nor do I find it suggested anywhere in the Portnoy references.” PO Resp. 31 (citing Ex. 2001 ¶ 99). However, we find such reliance to be unpersuasive because Mr. Jawadi simply parrots Patent Owner’s argument and provides little if any analysis of in support of Patent Owner’s disagreement. Instead, we credit and give greater weight to Dr. Srivastava’s declaration testimony that one of ordinary skill in the art would have understood that Portnoy discloses or suggests storing individual components in its dataset. *See* Ex. 1002 at ¶176–183.

However, to the extent that Portnoy does not disclose “storing individual components of said network packets in a database,” Petitioner contends that it would have been obvious to one of ordinary skill in the art “to store individual components in a database such as a Microsoft Access™ database in view of Cannady’s teaching.” Pet. 43 (citing Ex. 1002 ¶¶ 184–195); *see also* Pet. 43 (citing Ex. 1012 (“Cannady discloses that 100,000 individual events where [sic – were] stored in a Microsoft Access™ database.”)). According to Petitioner one of ordinary skill in the art “would have understood that Cannady’s database stores individual components of the network packets.” Pet. 43–44 (citing Ex. 1002 ¶ 193–195).

Based on the above, Petitioner concludes that the combination of Portnoy and Cannady discloses or renders obvious the argued limitation. Pet. 44 (Citing Ex. 1002 ¶¶ 196–204). Petitioner explains that “Portnoy

IPR2020-00879

Patent 7,260,846 B2

combined with the teachings of Cannady results in using a commercially available database for storing Portnoy's individual components of network packets." *Id.* Petitioner provides several reasons why "[a] POSITA would have been motivated to apply the teachings of Cannady's commercially available database to Portnoy's IDS to facilitate improved data management and retention." Pet. 44–46 (citing Ex. 1002 ¶¶ 198, 200–204; Ex. 1004, 18:48–63, 20:59–21:4; Ex. 1005, 4–7, 13; Ex. 1012, 5–6, 8).

In response, Patent Owner contends that "Cannady discusses databases a single time in its disclosure" and "does not disclose storing individual components of networks packets in a database." PO Resp. 31; Sur-Reply 7–8.<sup>14</sup> Patent Owner also argues that "Petitioner does not explain how using pieces of network data renders obvious the step of storing individual components of said packets in a database obvious." Sur-Reply 7 (citing Ex. 2002 ¶¶ 36, 50, 65, 73, 99).

Patent Owner's arguments do not undermine Petitioner's showing. At the outset, Petitioner's obviousness approach adequately identifies how the combination of Portnoy and Cannady renders obvious limitation [7.C], and is supported by citation to Dr. Srivastava's declaration testimony. Pet. 43–46 (citing Ex. 1002 ¶¶ 184–204). There is no dispute as to whether Cannady discloses storing data in a database. *See* Ex. 1012, 7 ("Approximately 10000 individual events were collected by RealSecure™ and stored in a Microsoft Access™ database, of which approximately 3000 were simulated attacks."). Instead, Patent Owner asserts that Cannady discloses "storing "events"

---

<sup>14</sup> Patent Owner also argues that Barbara fails to disclose limitation [7.C]. PO Resp. 31. However, Petitioner does not rely on Barbara to address limitation [7.C] (Pet. 41), and as such, we do not address Patent Owner's arguments directed to whether Barbara discloses limitation [7.C].

IPR2020-00879

Patent 7,260,846 B2

collected by RealSecure in a Microsoft Access database. PO Resp. 31 (citing Ex. 1012, 7). However, we credit the declaration testimony of Dr. Srivastava for the understanding that the “events” in Cannady “are each just a record of a packet broken down into its individual components.” Ex. 1002 ¶ 185. Thus, we agree with Petitioner that one of ordinary skill in the art “would have understood that Cannady’s database stores individual components of the network packets,” as claim 7 requires. Pet. 43–44 (citing Ex. 1002 ¶ 193–195).

For these reasons, Petitioner persuasively shows that “Portnoy, alone or in combination with Cannady, discloses, or at least renders obvious, Element [7.C].”

- e) *“Element [7.D]: constructing multi-dimensional vectors from at least two of said stored individual components and applying at least one multi-variate analysis to said constructed multi-dimensional vectors, said at least one multi-variate analysis producing a corresponding output set”*

Petitioner contends that “Portnoy discloses or renders obvious this limitation.” Pet. 46–49. For example, Petitioner asserts that

Portnoy discloses obtaining a “data instance (feature vector)” (*multi-dimensional vectors*) from the KDD Cup 1999 dataset and discloses an example of a feature vector having three features. Ex. 1005 at pp. 4–5, 7; *see also* Ex. 1004 at 11:54–12:52, 13:8–10. Further, Portnoy’s feature vectors are multidimensional because Portnoy teaches normalizing vectors to avoid bias caused by different feature scales, which does not occur in single dimensional feature vectors with only one scale. Ex. 1005 at pp. 4–5; *see also* Ex. 1004 at 11:54–12:53; Ex. 1002 at ¶208. And as mentioned, Portnoy gives an example of a feature vector with three features. Ex. 1005 at pp. 4–5, Ex. 1004 at 11:54–12:52.

Pet. 47. And, according to Petitioner, one of ordinary skill in the art

would have understood that Portnoy obtains multi-dimensional vectors from at least two of said stored individual components

constructed from the raw network traffic because a feature vector is a set of features which represent some object, such as a TCP connection or packet; in addition, Portnoy discloses a three-feature vector in an example. *See id.*; Ex. 1002 at ¶¶206–208; *see also* Ex. 1023 at Fig. 3 (illustrating that a feature vector is made up of feature elements), 19:52–20:18 (claiming constructing a multidimensional feature vector from data representing a gesture and using the vector in neural network analysis).

Pet. 47–48. Petitioner further asserts that “Portnoy applies a simple variant of single-linkage clustering (*at least one multi-variate analysis*) to a feature vector (*multi-dimensional vectors*).” Pet. 48 (citing Ex. 1002 ¶¶ 209–210; Ex. 1005, 5–6). And, with respect to “producing a corresponding output set,” Petitioner explains that one of ordinary skill in the art “would have understood that variants of single-linkage clustering produce a set of clusters (*a corresponding output set*).” Pet. 49 (citing Ex. 1005, 5–6; Ex. 1002 ¶ 209); *see also* Pet. 49 (“A POSITA would have understood that to obtain the multi-dimensional vectors, they are constructed.”) (citing Ex. 1002 ¶ 211).

Petitioner additionally asserts that “Cannady shows an example of selecting certain elements from a database record and further constructing them.” Pet. 49 (citing Ex. 1012, 8; Ex. 1002 ¶¶ 211–215).

We find that Petitioner’s contentions regarding this limitation, which Patent Owner does not dispute, are persuasive.

*f) “Element [7.E]: establishing a correlation between individual output sets based upon a selected metric to identify anomalous behavior”*

Petitioner contends that “Portnoy discloses, or at least renders obvious, Element [7.E].” Pet. 49–52. For example, Petitioner asserts that “Portnoy *establishes a correlation* in an individual output set, produced by

IPR2020-00879

Patent 7,260,846 B2

Portnoy's clustering methodology, based on whether they are part of some N percentage of largest clusters (N being the *selected metric*).” Pet. 50 (citing Ex. 1002 ¶¶ 226–228; Ex. 1005, 6; Ex. 1004, 13:47–51). Petitioner further asserts that

Portnoy determines some percentage N (selected metric) of the clusters containing the largest number of instances and marks them as normal (establishing a correlation). Ex. 1005 at p. 6; Ex. 1004 at 13:47–51; *see also* Ex. 1002 at ¶¶226–228. The remaining clusters are labeled as anomalous (establishing a correlation). Ex. 1005 at p. 6; Ex. 1004 at 13:47–51. Which clusters are correlated as anomalous and which are correlated as normal depends on what N is used (establishing a correlation between individual output sets based upon a selected metric) and Portnoy discloses various examples of a possible N. Ex. 1005 at p. 8; *see also* Ex. 1002 at ¶¶226–228[.]

Pet. 50.

We find that Petitioner's contentions regarding this limitation, which Patent Owner does not dispute, are persuasive.

- g) “*Element [7.F]: classifying said anomalous behavior as an event selected from the group consisting of a network fault, a change in network performance and a network attack.*”

Petitioner contends that “Portnoy alone, or combined with Barbara, discloses, or at least render obvious, Element [7.F].” Pet. 52–57. For example, Petitioner asserts that Portnoy's method “help[s] analysts focus on portions of the data that are more likely to contain intrusions.” Pet. 52 (citing Ex. 1005, 13). According to Petitioner, one of ordinary skill in the art

would have understood that the analysts would review the data and determine if the identified portion of data (*said anomalous behavior*) is an intrusion (*an event selected from the group consisting of... a network attack*) or some acceptable deviation from normal behavior because that is the nature of an analyst's

role in reviewing data or at the very least a common, well-known aspect of an analyst's role.

Pet. 52 (citing Ex. 1002 ¶¶ 232–233).

However, to the extent that Portnoy does not disclose “classifying said anomalous behavior as an event,” Petitioner contends that one of ordinary skill in the art “would have found it obvious to classify, as taught by Barbara, the identified anomalous data instances (anomalous behavior) of Portnoy.” Pet. 53 (citing Ex. 1002 ¶¶ 236–248) (emphasis omitted).

Petitioner asserts that

Barbara discloses the ADAM anomaly detection system, which includes . . . a classifier that uses a decision tree to determine (*classifying*) whether anomalous behavior (*said anomalous behavior*) is a deviating normal instance, a known attack (*network attack*), which are labeled with their attack type, or an unknown attack (*network attack*).

Pet. 53 (citing Ex. 1013, 3–5; Ex. 1002 ¶¶ 237–239). Petitioner further asserts that “Barbara discloses using ‘a Naive Bayes classifier to classify the instances into normal instances, known attacks and new attacks.’” Pet. 54 (citing Ex. 1013, 2) (emphasis omitted).

Based on the above, Petitioner concludes that “Portnoy in combination with Barbara discloses or renders obvious Element [7.F] by applying the teachings of Barbara’s classifiers to review Portnoy’s detected anomalies and sort out attacks from permissible deviations.” Pet. 55 (citing Ex. 1002 ¶¶ 230, 245–247); *see also id.* at 56 (citing Ex. 1002 ¶¶ 240–248 (“Barbara’[s] teachings would build on Portnoy because Barbara’s classifiers would act as a second line of defense by sorting and classifying Portnoy’s detected anomalies.”)). Petitioner provides several reasons why “[a] POSITA would have been motivated to combine the teachings of Barbara’s . . . with Portnoy’s IDS.” Pet. 55–57 (citing Ex. 1002 ¶¶ 240–248;

IPR2020-00879

Patent 7,260,846 B2

Ex. 1004, 1:52–64, 4:31–42; Ex. 1005, Abstract; Ex. 1013, 2–3). For example, Petitioner asserts that one of ordinary skill in the art “would have been motivated to incorporate either classification approach of Barbara to automate Portnoy’s manual approach, and reduce the false positives rates, and/or proactively determine that nature of the attack.” *Id.* at 55 (citing Ex. 1013, 2–3; Ex. 1002 ¶¶ 241–242).

We find that Petitioner’s contentions regarding this limitation, which Patent Owner does not dispute, are persuasive.

#### 6. *Analysis of Claim 8*

Claim 8 depends from claim 7, and further recites “wherein said storing step comprises the steps of: identifying protocol boundaries in each extracted network packet; and, storing data from each field separated by said identified protocol boundaries in a separate record in said database.”

Petitioner contends that “Portnoy in view of Cannady discloses, or at least renders obvious,” claim 8. Pet. 57–60. Petitioner persuasively maps the limitations of dependent claim 8 to the cited art with support provided by the declaration testimony of Dr. Srivastava. *Id.* (citing Ex. 1002 ¶¶ 185, 252–253, 258–261, 263–271; Ex. 1012, 7–8; Ex. 1018; Ex. 1019; Ex. 1020).

We find Petitioner’s arguments and evidence, which Patent Owner does not dispute, are persuasive. We determine, for the reasons expressed by Petitioner, that the combination of Portnoy and Cannady teaches or suggests the limitations of claim 8 and that one of ordinary skill in the art would have been motivated to combine the references in the manner proposed by Petitioner.

For the foregoing reasons, we determine that Petitioner has demonstrated by a preponderance of the evidence that claim 8 would have been obvious in view of Portnoy and Cannady.

### 7. Conclusion (Ground 1)

Having considered the parties' arguments and evidence, we find Petitioner has demonstrated persuasively that the teachings of Portnoy and Cannady and/or Barbara have been properly combined and one of ordinary skill in the art would have found it obvious to combine these teachings in the manner proposed by Petitioner.

Therefore, after having analyzed the entirety of the record and assigning appropriate weight to the cited supporting evidence, we determine Petitioner has shown by a preponderance of the evidence that claims 7 and 8 are unpatentable over the combination of Portnoy, Cannady, and Barbara.

### E. Alleged Obviousness over Portnoy, Cannady, Barbara, and AAPA (Ground 2: Claims 10 and 11)

Petitioner contends that claims 10 and 11 are unpatentable as obvious over Portnoy, Cannady, Barbara, and AAPA. Pet. 60–70. Petitioner also relies on the testimony of Dr. Srivastava to support its arguments. *Id.*

#### 1. Overview of AAPA (Ex. 1001)

Petitioner asserts that “the '846 patent admits ‘well-known principal component analysis can be applied to the multi-dimensional vectors in order to facilitate the reduction of the multi-dimensional vectors.’” Pet. 61 (citing Ex. 1001, 9:4–7).<sup>15</sup>

---

<sup>15</sup> “[A]dmissions by the applicant in the specification of the challenged patent standing alone cannot be used as the basis for instituting an IPR,” but “[s]tatements in a challenged patent’s specification may be used . . . when they evidence the general knowledge possessed by someone of ordinary skill in the art” if used “in conjunction with one or more prior art patents or printed publications forming ‘the basis’ of the proceeding under § 311.” USPTO Memorandum, Treatment of Statements of the Applicant in the Challenged Patent in Inter Partes Reviews Under § 311 (August 18, 2020) 4,

## 2. Analysis of Claim 10

Claim 10 follows:

The method of claim 7, wherein said step of applying at least one multi-variate analysis to said constructed multi-dimensional vectors comprises the steps of: reducing said constructed multi-dimensional vectors; and, applying at least one self-organizing clustering methodology to said reduced multi-dimensional vectors, said application of said at least one self-organizing clustering methodology producing a corresponding output set of clusters.

Ex. 1001, 12:7–16.

Petitioner contends that “Portnoy in view of AAPA discloses, or at least renders obvious,” claim 10. Pet. 60–66. Petitioner persuasively maps the limitations of dependent claim 10 to the cited art with support provided by the declaration testimony of Dr. Srivastava. *Id.* (citing Ex. 1001, 9:4–7; Ex. 1002 ¶¶ 279–286, 288–292; Ex. 1004, 11:54–12:53, 13:8–14:27; Ex. 1005, 3–7; Ex. 1021, 13:25–38, 13:65–14:20; Ex. 1022, 12, Fig. 4).

We find that Petitioner’s arguments and evidence, which Patent Owner does not dispute, are persuasive. We determine, for the reasons expressed by Petitioner, that the combination of Portnoy and AAPA teaches or suggests the limitations of claim 10 and that one of ordinary skill in the art would have been motivated to combine the references in the manner proposed by Petitioner.

## 3. Analysis of Claim 11

Claim 11 recites:

The method of claim 10, wherein said establishing step comprises the steps of: loading at least one selectable metric; correlating individual ones of said clusters in said output set;

---

*available at https://www.uspto.gov/sites/default/files/documents/signed\_aapa\_guidance\_memo.pdf (“§ 311 Memorandum”).*

determining whether any of said correlations deviate from said loaded at least one selectable metric; and, for each one of said correlated clusters in said output set which deviates from said loaded at least one selectable metric, labeling said deviating correlated cluster as exhibiting anomalous behavior.

Ex. 1001, 12:17–29.

Petitioner contends that “Portnoy discloses, or renders obvious,” claim 11. Pet. 66–70. Petitioner persuasively maps the limitations of dependent claim 11 to the cited art with support provided by the declaration testimony of Dr. Srivastava. *Id.* (citing Ex. 1002 ¶¶ 206, 296–298, 300–302, 304–312; Ex. 1004 at 13:32–51; Ex. 1005, 2–3, 6–8).

We find that Petitioner’s arguments and evidence, which Patent Owner does not dispute, are persuasive. We determine, for the reasons expressed by Petitioner, that the combination of Portnoy teaches or suggests the limitations of claim 11 and that one of ordinary skill in the art would have understood the references in the manner proposed by Petitioner.

#### 4. *Conclusion (Ground 2)*

Having considered the parties’ arguments and evidence, we determine that Petitioner has demonstrated persuasively that the teachings of Portnoy, Cannady, Barbara, and AAPA have been properly combined and one of ordinary skill in the art would have found it obvious to combine these teachings in the manner proposed by Petitioner.

Therefore, after having analyzed the entirety of the record and assigning appropriate weight to the cited supporting evidence, we determine Petitioner has shown by a preponderance of the evidence that claims 10 and 11 are unpatentable over the combination of Portnoy, Cannady, Barbara, and AAPA.

#### IV. PETITIONER'S MOTION TO EXCLUDE

Petitioner filed a motion to exclude certain paragraphs of Mr. Jawadi's declaration (Ex. 2001). Mot. 3–9. Petitioner asserts that paragraphs 51, 55, 56, 60–63, 75, 82–87, 96–98, and 103–149 of Mr. Jawadi's declaration should be excluded because Patent Owner does not cite to them. *Id.* at 2–3. Petitioner further asserts that paragraphs 50, 52, 53, 58, 59, 65–74, 76, and 77 of Mr. Jawadi's declaration should be excluded because they “are either verbatim or near verbatim duplication of the [Patent Owner Response] and are only cited in passing in Patent Owner’s Sur-Reply.” *Id.* at 7. Patent Owner filed an Opposition to Petitioner’s Motion (Opp.), and Petitioner filed a Reply in support of its Motion (Reply).

Although we may have explicitly or implicitly referenced these exhibits when recounting or addressing the parties’ arguments, we do not rely on any of the referenced paragraphs as a basis to make any findings adverse to Petitioner in this Decision. We, therefore, dismiss Petitioner’s Motion to Exclude as moot.

Our general approach for considering challenges to the admissibility of evidence was outlined in *Corning Inc. v. DSM IP Assets B.V.*, IPR2013-00053, Paper 66 at 19 (PTAB May 1, 2014). As stated in *Corning*, similar to a district court in a bench trial, the Board, sitting as a non-jury tribunal with administrative expertise, is well-positioned to determine and assign appropriate weight to evidence presented. *Id.* (citing *Donnelly Garment Co. v. NLRB*, 123 F.2d 215, 224 (8th Cir. 1941) (stating, in the context of reviewing an administrative determination of the National Labor Relations Board based on findings by a Trial Examiner, “[w]e think that experience has demonstrated that in a trial or hearing where no jury is present, more time is ordinarily lost in listening to arguments as to the admissibility of

IPR2020-00879

Patent 7,260,846 B2

evidence and in considering offers of proof than would be consumed in taking the evidence proffered . . . . One who is capable of ruling accurately upon the admissibility of evidence is equally capable of sifting it accurately after it has been received . . . .”)).

Moreover, “there is a strong public policy for making all information filed in an administrative proceeding available to the public.” *Liberty Mut. Ins. Co. v. Progressive Cas. Ins. Co.*, CBM2012-00010, Paper 59 at 40 (PTAB Feb. 24, 2014). Rather than excluding evidence that is allegedly hearsay, confusing, misleading, untimely, and/or irrelevant, we simply do not rely on it or give it little or no probative weight.

V. CONCLUSION<sup>16</sup>

In summary:

Claims	35 U.S.C. §	Reference(s)/Basis	Claims Shown Unpatentable	Claims Not shown Unpatentable
7, 8	103(a)	Pornoy, Cannady, Barbara	7, 8	
10, 11	103(a)	Pornoy, Cannady, Barbara, AAPA	10, 11	
<b>Overall Outcome</b>			7, 8, 10, 11	

## VI. ORDER

For the reasons given, it is:

ORDERED that Petitioner has established based on a preponderance of evidence that claims 7, 8, 10, and 11 of U.S. Patent 7,260,846 B2 are *unpatentable* as set forth above;

FURTHER ORDERED that Petitioner's Motion to Exclude is *dismissed*; and

FURTHER ORDERED because this is a final written decision, the parties to this proceeding seeking judicial review of our Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

---

<sup>16</sup> Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. § 42.8(a)(3), (b)(2).

IPR2020-00879

Patent 7,260,846 B2

For PETITIONER:

David Tenant  
ALLEN & OVERY LLP  
[David.tenant@allenovery.com](mailto:David.tenant@allenovery.com)

David Markoff  
WHITE & CASE LLP  
[David.markoff@whitecase.com](mailto:David.markoff@whitecase.com)

Roshan Mansinghani  
Jung Hahm  
UNIFIED PATENTS, LLC  
[roshan@unifiedpatents.com](mailto:roshan@unifiedpatents.com)  
[jung@unifiedpatents.com](mailto:jung@unifiedpatents.com)

For PATENT OWNER:

Vincent Rubino  
FABRICANT LLP  
[vrubino@fabricantllp.com](mailto:vrubino@fabricantllp.com)

John Rubino  
RUBINO LAW LLC  
[jarubino@rubinoip.com](mailto:jarubino@rubinoip.com)



(12) **United States Patent**  
**Day**

(10) **Patent No.:** **US 7,260,846 B2**  
(b5) **Date of Patent:** **\*Aug. 21, 2007**

(54) **INTRUSION DETECTION SYSTEM**

(75) Inventor: **Christopher W. Day**, Biscayne Park, FL (US)

(73) Assignee: **Steelcloud, Inc.**, Herndon, VA (US)

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **11/367,950**

(22) Filed: **Mar. 3, 2006**

(65) **Prior Publication Data**

US 2006/0156404 A1 Jul. 13, 2006

(51) **Int. Cl.**

**G06F 11/00** (2006.01)

(52) **U.S. Cl.** ..... **726/23; 726/11; 726/13; 726/14; 726/25; 726/27; 713/194; 709/223**

(58) **Field of Classification Search** ..... **726/23, 726/11, 13-14, 25, 27; 713/194; 709/223**

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,278,901 A 1/1994 Shieh et al. ..... 380/4  
5,311,593 A 5/1994 Carmi ..... 380/23  
5,414,833 A 5/1995 Hershey et al. ..... 395/575

(Continued)

FOREIGN PATENT DOCUMENTS

EP 0 985 995 3/2000

(Continued)

OTHER PUBLICATIONS

Roesch, Snort—Lightweight Intrusion Detection for Networks, 1999, Usenix, pp. 1-2.\*

(Continued)

Primary Examiner—Kim Vu

Assistant Examiner—Paula Klimach

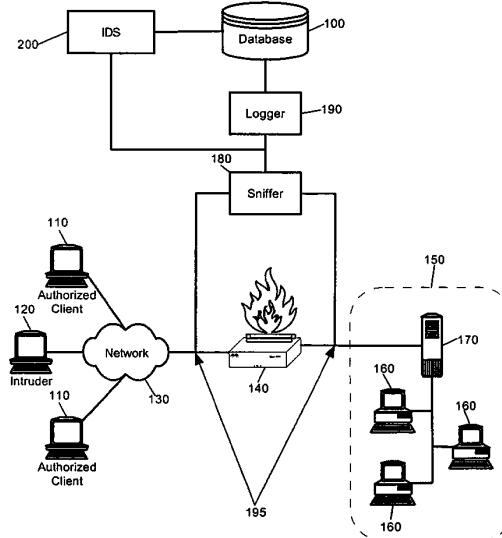
(74) Attorney, Agent, or Firm—Steven M. Greenberg, Esq.

(57)

**ABSTRACT**

An intrusion detection system (IDS). An IDS which has been configured in accordance with the present invention can include a traffic sniffer for extracting network packets from passing network traffic; a traffic parser configured to extract individual data from defined packet fields of the network packets; and, a traffic logger configured to store individual packet fields of the network packets in a database. A vector builder can be configured to generate multi-dimensional vectors from selected features of the stored packet fields. Notably, at least one self-organizing clustering module can be configured to process the multi-dimensional vectors to produce a self-organized map of clusters. Subsequently, an anomaly detector can detect anomalous correlations between individual ones of the clusters in the self-organized map based upon at least one configurable correlation metric. Finally, a classifier can classify detected anomalous correlations as one of an alarm and normal behavior.

**12 Claims, 4 Drawing Sheets**



## US 7,260,846 B2

Page 2

## U.S. PATENT DOCUMENTS

5,526,299 A	6/1996	Coifman et al. ....	364/807
5,621,889 A	4/1997	Lermuzeaux et al. ....	395/186
5,692,124 A	11/1997	Holden et al. ....	395/187.01
5,787,253 A	7/1998	McCreery et al. ....	395/200.61
5,835,726 A	11/1998	Shwed et al. ....	395/200.59
5,850,386 A	12/1998	Anderson et al. ....	370/241
5,918,223 A	6/1999	Blum et al. ....	707/1
5,968,176 A	10/1999	Nessett et al. ....	713/201
5,991,881 A	11/1999	Conklin et al. ....	713/201
6,026,442 A	2/2000	Lewis et al. ....	709/229
6,044,401 A	3/2000	Harvey ....	709/225
6,088,804 A	7/2000	Hill et al. ....	713/201
6,115,393 A	9/2000	Engel et al. ....	370/469
6,134,664 A	10/2000	Walker ....	713/291
6,263,444 B1	7/2001	Fujita ....	713/201
6,279,113 B1	8/2001	Vaidya ....	713/201
6,282,546 B1	8/2001	Gleichauf et al. ....	707/102
6,301,668 B1	10/2001	Gleichauf et al. ....	713/201
6,304,262 B1	10/2001	Maloney et al. ....	345/418
6,304,904 B1	10/2001	Sathyaranayanan et al. ....	709/224
6,321,338 B1	11/2001	Porras et al. ....	713/201
6,327,550 B1	12/2001	Vinberg et al. ....	702/186
2002/0032880 A1	3/2002	Poletto et al. ....	714/4
2002/0035683 A1	3/2002	Kaashoek et al. ....	713/154

## FOREIGN PATENT DOCUMENTS

WO	WO 00/34847	6/2000
----	-------------	--------

## OTHER PUBLICATIONS

G. Bigna, et al., NetSTAT: A Network-based Intrusion Detection Approach, *Proc. of the 14th Annual Computer Security Application Conf.*, Scottsdale, AZ, (Dec. 1998).

C. Prosiise, et al., *Catch Hackers in the Act*, <<http://builder.cnet.com/webbuilding/0-7532-8-4011019-4.html>>, (Dec. 13, 2000).

*The Science of Intrusion Detection System Attack Identification*, Cisco Systems, Inc., (2002).

C. Gerg, A Platform-Independent Discussion of Network Security, *Information Security Bulletin*, pp. 29-33, (May 2001).

A. Allan, Intrusion Detection Systems (IDSs): Perspective, *Gartner*, (Jan. 4, 2002).

*Snort Overview*, <[http://www.snort.org/docs/writing\\_rules.chap1.html](http://www.snort.org/docs/writing_rules.chap1.html)>, (Jul. 15, 2002).

W. Simonds, *Bad Packets: Snort—The Dobermans Behind the Firewall*, searchNetworking.com, (Feb. 28, 2002).

Roundtable—IDS At the Crossroads, *Information Security Magazine*, (Jun. 2002).

E. Duggan, Hackers Warn of 'Crackers', *The South Florida Business Journal*, (Jul. 5-11, 2002).

\* cited by examiner

U.S. Patent

Aug. 21, 2007

Sheet 1 of 4

US 7,260,846 B2

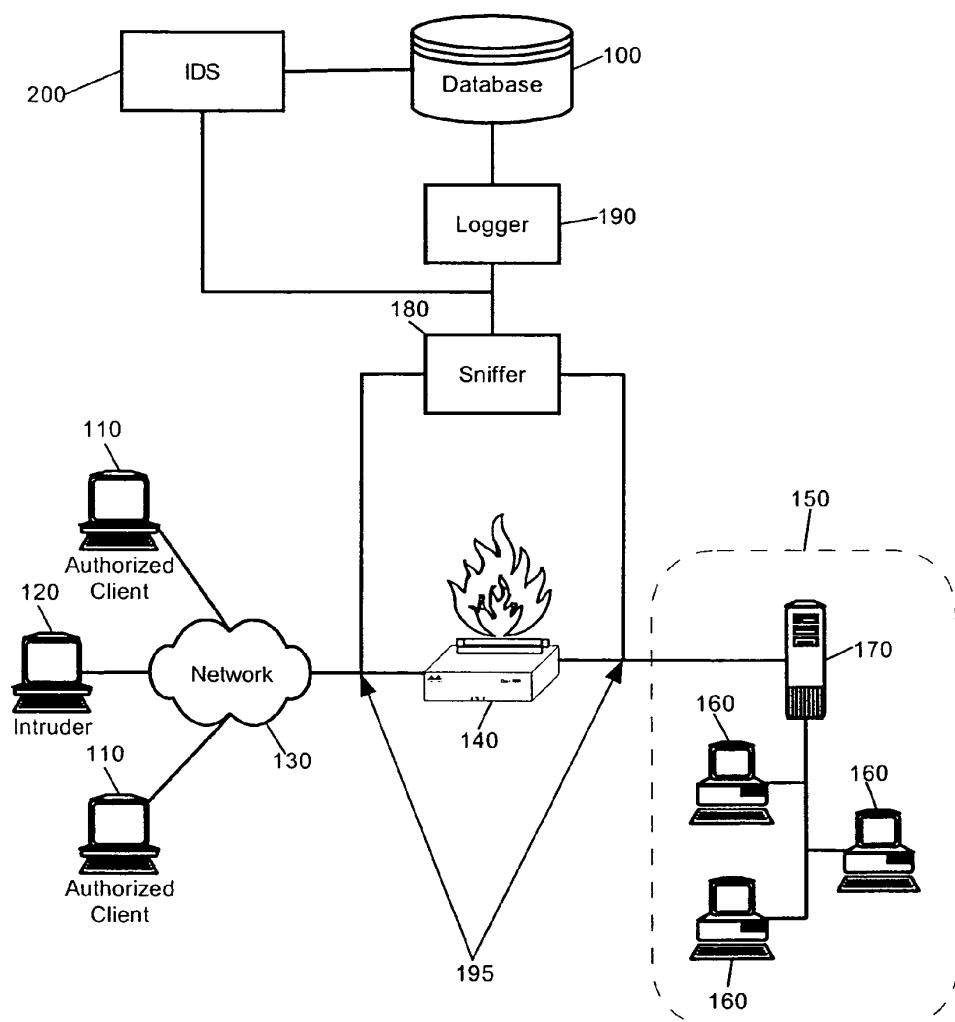


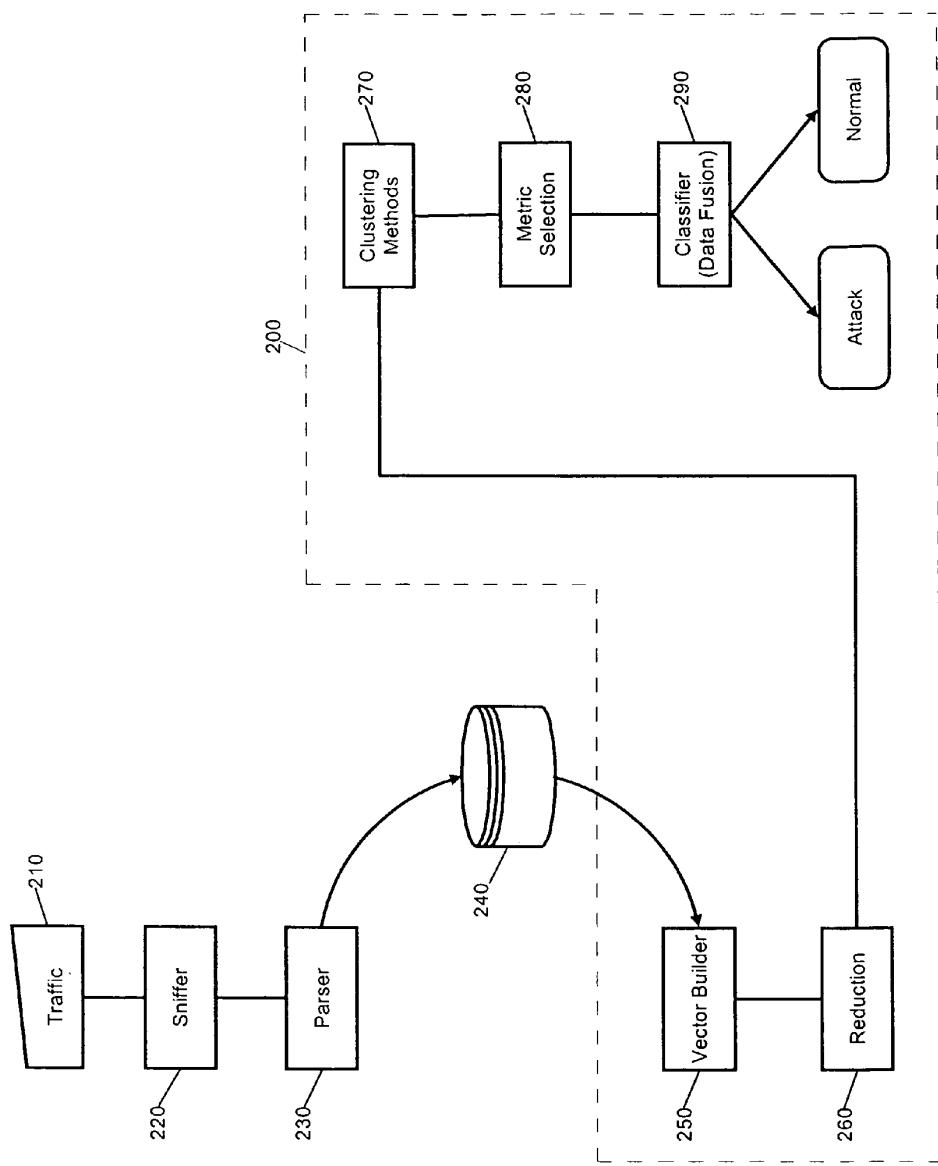
FIG. 1

U.S. Patent

Aug. 21, 2007

Sheet 2 of 4

US 7,260,846 B2



**FIG. 2**

U.S. Patent

Aug. 21, 2007

Sheet 3 of 4

US 7,260,846 B2

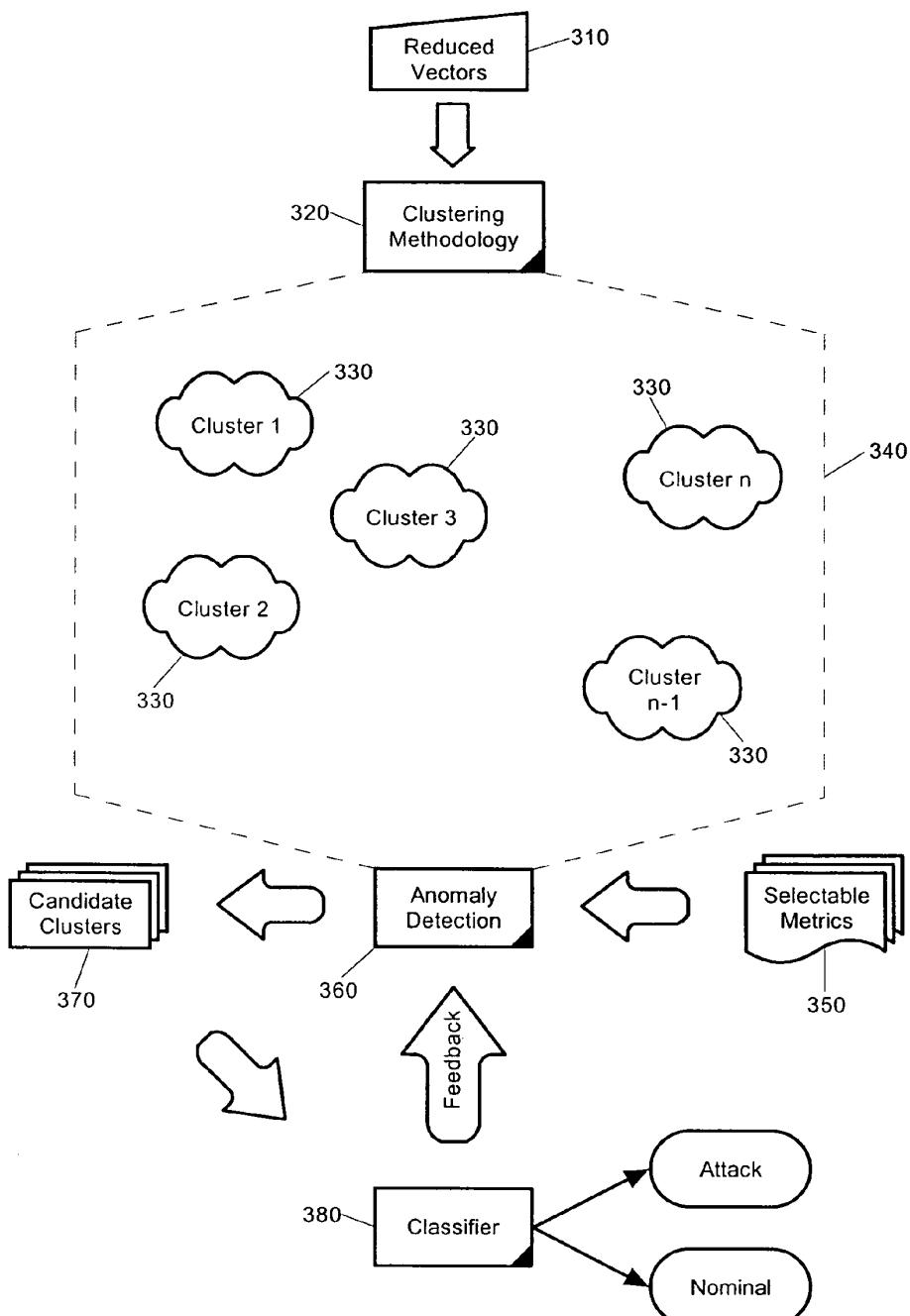


FIG. 3

U.S. Patent

Aug. 21, 2007

Sheet 4 of 4

US 7,260,846 B2

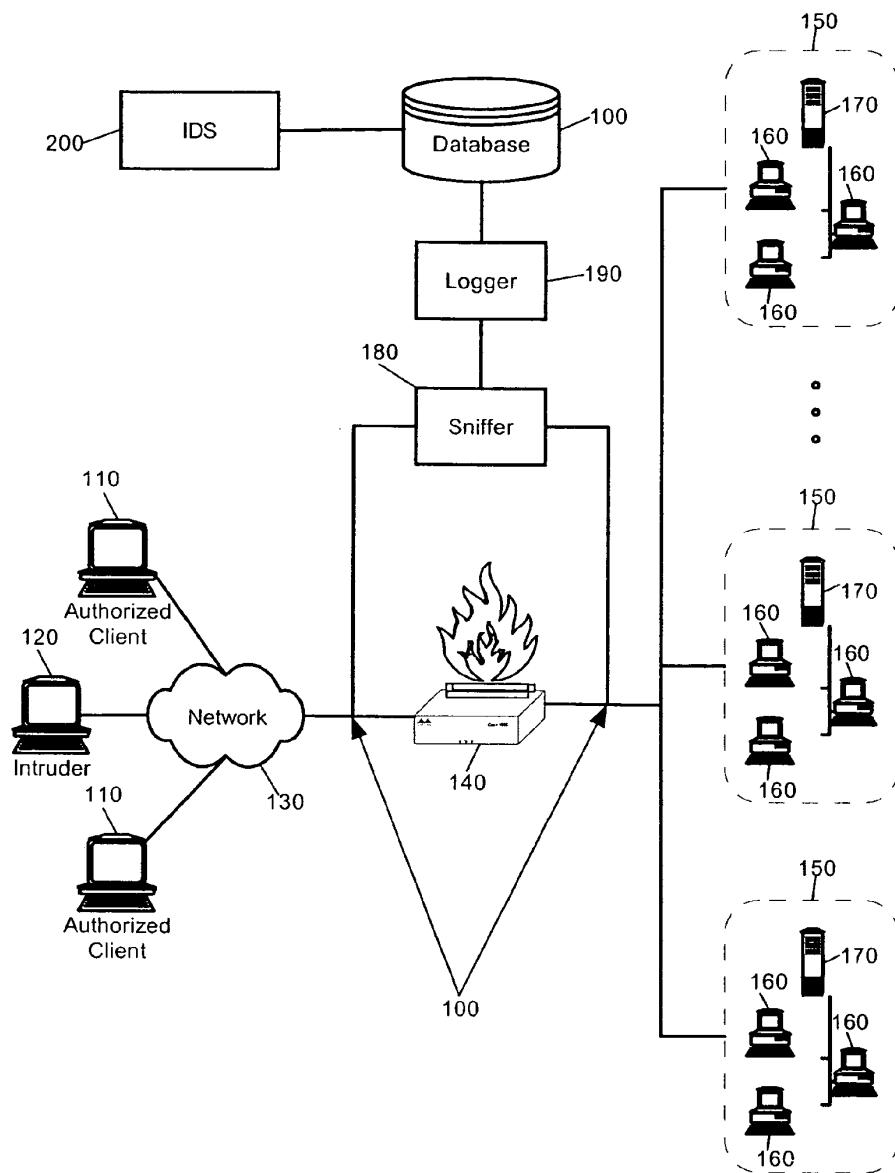


FIG. 4

US 7,260,846 B2

**1****INTRUSION DETECTION SYSTEM****BACKGROUND OF THE INVENTION****1. Statement of the Technical Field**

The present invention relates to computer communications network security and performance monitoring and more particularly to an intrusion detection system.

**2. Description of the Related Art**

Internet security has increasingly become the focus of both corporate and home computer users who participate in globally accessible computer networks. In particular, with the availability of broadband Internet access, even within smaller computer communication networks, most network attached computing devices enjoy continuous access to the Internet. Notwithstanding, continuous, high-speed access is not without its price. Specifically, those computers and computer networks which heretofore had remained disconnected from the security risks of the Internet now have become the primary target of malicious Internet hackers, crackers and script kiddies (relatively unskilled hackers), collectively referred to herein as "unauthorized intruders".

Notably, many such unauthorized intruders continuously scan the Internet for Internet Protocol (IP) addresses and ports of vulnerable computers communicatively linked to the Internet. At the minimum, those vulnerable computers can experience nuisance damage such as accessed, deleted or modified files or defaced Web pages. Yet, at the other extreme, for the unsuspecting end-user, their computer can become the launching pad for more malicious attacks which can cripple whole segments of the Internet.

To combat the enhanced threat of unauthorized intruders, information technologists have liberally deployed firewall technology about the enterprise, at least to limit the source and channel of packet flow to and from the enterprise. Still, while firewall usage can limit the number of ports through which an unauthorized intruder can access an internal portion of a network, the firewall in of itself can be comprised by an unauthorized intruder. Popular examples include denial of service attacks and SYN flood attacks. Thus, while firewall usage can improve the security of a network, deploying firewall technology alone cannot completely secure the network.

To fill the security gap left open by firewall usage, information technologists incorporate intrusion detection system (IDS) technology within the enterprise. IDS technology can detect network intrusions dynamically as they occur or post-mortem after the intrusion has occurred. A typical dynamic network IDS, for instance the IDS disclosed in United States Patent Application Publication No. 2002/0035683 A1 to Kaashoek et al. for ARCHITECTURE TO THWART DENIAL OF SERVICE ATTACKS, can include a monitoring component able to capture network packets as the packets pass through the IDS, an inference component for determining whether the captured traffic indicates any malicious activity or usage, and a response component able to react appropriately to the detection of a malicious intrusion. While the response can include the generation and transmission of a simple e-mail message to a system administrator, the response also can include more complex actions, for instance temporarily blocking traffic flowing from an offenders Internet protocol (IP) address.

Conventional IDS technology can incorporate a variety of methodologies for determining within the inference component whether malicious activity has occurred or is occurring. Referred to as "detection methodologies", examples can include simple pattern matching, stateful pattern matching,

**2**

protocol decode-based signatures, heuristic-based signatures, and anomaly detection. Pattern matching is based upon inspecting traffic to identify a fixed sequence of bytes in a single packet. The fixed sequence of bytes, referred to in the art as a "signature", when identified within inspected traffic, can trigger an alarm. U.S. Pat. No. 6,279,113 B1 to Vaidya for DYNAMIC SIGNATURE INSPECTION-BASED NETWORK INTRUSION DETECTION illustrates an exemplary use of pattern matching technology.

Still, pattern matching is considered to be the most primitive of the detection methodologies employed in a typical IDS. In that regard, pattern matching can fail where the hack attack differs only slightly from the stored signatures leading to what is known as "false negatives"—the failure to detect an attack after having inspecting traffic associated with an attack. Stateful pattern matching is an enhanced, more mature version of simple pattern matching based upon the notion that a stream of network traffic includes more than mere stand-alone packets. In consequence, pattern matching ought to be applied in the context of a stream of packets. To place pattern matching within the context of a stream of packets, the stateful pattern matching methodology considers the arrival order of packets in a stream and applies pattern matching to packets in the stream. Still, like simple pattern matching, stateful pattern matching can fail where the pattern of an attack differs only slightly from the stored signatures, again leading to false negatives.

Protocol decode-based analysis has been considered to be an intelligent extension to stateful pattern matching. In protocol decode-based analysis, traffic first is decoded in real-time according to a specified protocol such as HTTP in order to identify the pertinent fields of the protocol. Once the fields of the traffic specified by the protocol have been decoded, pattern matching can be applied to the decoded fields. U.S. Pat. No. 6,301,668 B1 to Gleichauf et al. for METHOD AND SYSTEM FOR ADAPTIVE NETWORK SECURITY USING NETWORK VULNERABILITY ASSESSMENT illustrates one such application of a protocol decode-based analysis.

As will be apparent from a review of the '668 system, the protocol decode-based analysis can limit the number of false alarms, or "false positives", encountered during the matching process because much of the matched elements are placed into context through the decoding process. Still, the false positive rate of the protocol decode-based analysis is largely dependent on the accuracy of the publicly-specified protocol definition. Also, the success of the protocol decode-based analysis relies directly upon the freshness of the patterns used to identify unauthorized intrusions.

Unlike intrusion detection techniques which rely directly upon pattern matching, a heuristic-based analysis employs algorithmic logic upon which intrusion detection signatures can be based. Typically, the algorithmic logic can analyze traffic patterns in order to match a particular traffic pattern with a known "signature". For instance, the probing of a network device can be detected where many unique ports are accessed over a limited period of time. Moreover, the type of packets touching the unique ports further can indicate whether an unauthorized intrusion is unfolding. Of course, any heuristic-based analysis can report false positives where a pattern of legitimate access to a network device satisfies the algorithmic logic. Hence, the use of a heuristic-based analysis requires extensive and frequent tuning to limit such false positives.

Similar to the heuristic-based analysis, in an anomaly-based analysis, traffic can be dynamically inspected as the traffic passes through the IDS. In an anomaly-based analysis,

## US 7,260,846 B2

3

however, traffic patterns can be analyzed to detect anomalous behavior. Specifically, in an anomaly-based analysis, first a normal state is defined. Subsequently, traffic patterns which deviate from the normal state are labeled as unauthorized intrusions. Notably, though some anomaly-based analysis are configured to adapt the definition of normal state to traffic patterns as they unfold, none have been able to properly avoid the classification of some abnormal behavior as normal behavior. Moreover, no one conventional anomaly-based analysis has been able to distinguish anomalous behavior from permissible deviations from the normal state.

Nevertheless, IDS technology heretofore has been unable to provide a comprehensive method for detecting unauthorized intrusions while minimizing false positives. Specifically, static methods of detection such as pattern matching and its derivatives standing alone can be defeated by a sophisticated intruder with relative ease. Likewise, dynamic methods of detection such as those based upon heuristics and anomaly detection are limited to the extent that the methods can be configured improperly or ineffectively.

In addressing the deficiencies of the foregoing IDS methodologies, several IDS technologies incorporate a hybrid combination of static signature based pattern matching algorithms and dynamic anomaly detection algorithms. As an example, U.S. Pat. No. 6,321,338 to Porras et al. for NETWORK SURVEILLANCE discloses a method of network surveillance in which one or more analysis engines can perform both signature analysis and a statistical profiling of recorded network events. As discussed in column 4, lines 61 through 67 of the '338 specification, the event stream can be derived from a variety of sources, specifically the payload of a TCP/IP network packet or data contained in an analysis report.

Nevertheless, in view of the substantial processing resources required to reduce network traffic flowing across multiple network nodes, the '338 system processes only "events" detected and disseminated by a group of distributed monitoring components. That is to say, the '338 system does not process all network traffic flowing through the IDS with which the traffic can be analyzed to identify an unauthorized intrusion. Instead, the '338 system performs a tiered analysis of suspicious events in order to reduce the resource overhead which otherwise would be associated with a more thorough analysis.

More importantly, as the '338 system undertakes a fundamental analysis only of "event data" as stated in column 5, lines 34-35, the '338 system does not analyze traffic at a granular enough level to apply sophisticated statistical analyses. In particular, in the field of network analysis it is known to extract data from each individual packet field in a network packet in order to troubleshoot traffic flow in a network. U.S. Pat. No. 5,787,253 to McCreery et al. for APPARATUS AND METHOD OF ANALYZING INTERNET ACTIVITY describes such a device. Yet, in conventional IDS technology such as that described in the '338 system, the individual fields of a network traffic packet are never analyzed. In fact, in the '338 system, only the payload of an errant packet is extracted for analysis.

Ideally, to undertake the effective statistical analysis which is required to minimize false positives in the application of an anomaly based detection scheme, a maximum amount of data samples of exceptional granularity will be required. Thus, in the context of an IDS, it would be preferable to analyze each packet flowing across the IDS. Yet, to process each packet in-line would require an unreasonable share of processing resources. Moreover, to process

4

each packet in batch would require substantial fixed storage and an unusually thorough analysis scheme not available through ordinary anomaly based detection schemes.

As an example, the IDS taught in U.S. Pat. No. 6,282,546 to Gleichauf et al. for SYSTEM AND METHOD FOR REAL-TIME INSERTION OF DATA INTO A MULTI-DIMENSIONAL DATABASE FOR NETWORK INSTRUCTION DETECTION AND VULNERABILITY ASSESSMENT employs the batch processing of real-time acquired data to detect an unauthorized intrusion. Yet, the '546 system performs a limited analysis only upon a limited set of scalar meta-data such as time, address space, and event type. Moreover, the '546 system performs an analysis only upon a limited subset of all traffic passing through the IDS—namely data already associated with an event such as an attack. The '546 system, then, does not analyze any volume of network traffic prior to the detection of an event. Thus, the '546 system like other conventional IDS implementations, cannot achieve a high level of intrusion detection while minimizing false positives.

## SUMMARY OF THE INVENTION

The present invention is an IDS which overcomes the limitations of conventional IDS technology. Specifically, in the present invention, the IDS can monitor and packets passing across a coupled communications path. The IDS can identify protocol boundaries separating the various fields of each passing network packet and can store data for selected ones or all of the fields in a database, such as a relational database. In particular, data for each field can be stored in a separate record to facilitate the robust analysis of the stored data at a substantially granular level.

Once sufficient data has been stored in the database, multi-dimensional vectors can be constructed and reduced from the stored data. The reduced multi-dimensional vectors can be processed using one or more conventional multi-variate analysis methods and the output sets produced by the multi-variate analysis methods can be correlated against one another according to one or more selected metrics. Based upon these correlations, both normal and anomalous events can be identified.

An IDS which has been configured in accordance with the present invention can include a traffic sniffer for extracting network packets from passing network traffic; a traffic parser configured to extract individual data from defined packet fields of the network packets; and, a traffic logger configured to store individual packet fields of the network packets in a database. A vector builder can be configured to generate multi-dimensional vectors from selected features of the stored packet fields.

Notably, at least one self-organizing clustering module can be configured to process the multi-dimensional vectors to produce a self-organized map of clusters. Subsequently, an anomaly detector can detect anomalous correlations between individual ones of the clusters in the self-organized map based upon at least one configurable correlation metric. Finally, a classifier can classify detected anomalous correlations as either an alarm or normal behavior.

In one aspect of the present invention, the self-organizing clustering module can be configured to perform at least one of a Kohonen self-organizing map analysis, a principal component analysis, a multi-dimensional scaling analysis, a principal curve analysis, a wavelet analysis, and a neural network analysis. Also, the correlation metric can be configured either heuristically or manually. For example, the correlation metric can be a distance metric selected from the

## US 7,260,846 B2

## 5

group consisting of a Euclidean distance metric and a non-Euclidean distance metric. Finally, the classifier can be configured to weight individual ones of the anomalous correlations according to a corresponding self-organizing clustering module used to produce particular clusters between which the individual ones of the anomalous correlations are detected.

An intrusion detection method also can be provided in accordance with the inventive arrangements. The method can include the steps of monitoring network traffic passing across a network communications path; extracting network packets from the passing traffic; and, storing individual components of the network packets in a database. Multi-dimensional vectors can be constructed from at least two of the stored individual components and at least one multi-variate analysis can be applied to the constructed multi-dimensional vectors. In consequence, the multi-variate analysis can produce a corresponding output set;

A correlation can be established between individual output sets based upon a selected metric to identify anomalous behavior. As such, the anomalous behavior can be classified as one of a network fault and a network attack. Importantly, the storing step can include both identifying protocol boundaries in each extracted network packet; and, storing data from each field separated by the identified protocol boundaries in a separate record in the database. Moreover, with each individual component in the separate record in the database, data can be stored which associates the individual component with at least one of a corresponding target network device, a corresponding network socket, and a corresponding customer in a managed service provider environment.

The step of applying at least one multi-variate analysis to the constructed multi-dimensional vectors can include both reducing the constructed multi-dimensional vectors; and, applying at least one self-organizing clustering methodology to the reduced multi-dimensional vectors. In that regard, the application of the at least one self-organizing clustering methodology can produce a corresponding output set of clusters. In consequence, in the establishing step at least one selectable metric can be loaded and individual ones of the clusters in the output set can be correlated. It can be determined whether any of the correlations deviate from the loaded at least one selectable metric. Finally, for each one of the correlated clusters in the output set which deviates from the loaded at least one selectable metric, the deviating correlated cluster can be labeled as exhibiting anomalous behavior.

Importantly, the IDS of the present invention can be disposed according to a managed service provider model. In that regard, the IDS can be coupled to multiple communications paths leading to separate network domains belonging to or managed by separate customers. In this regard, the intrusion detection method of the present invention can include monitoring network traffic passing across a network communications path destined for multiple target devices in multiple independent network domains and extracting network packets from the passing traffic.

Protocol boundaries can be identified in each extracted network packet and data from each field separated by the identified protocol boundaries can be stored in a separate record in a database. The data in the database can be associated with at least one of a corresponding target device, a target network domain, a target customer, and a target customer sub-net. Subsequently, the stored data can be processed using at least one multi-variate clustering method to establish correlations between fields of different network

## 6

5 packets destined for different ones of the multiple independent network domains. Finally, a network attack can be identified based upon the established correlations.

## BRIEF DESCRIPTION OF THE DRAWINGS

There are shown in the drawings embodiments which are presently preferred, it being understood, however, that the invention is not limited to the precise arrangements and 10 instrumentalities shown, wherein:

FIG. 1 is a schematic illustration of a private network 15 configured with IDS technology in accordance with the inventive arrangements;

FIG. 2 is a flow chart illustrating a process for performing 15 intrusion detection using the IDS technology of FIG. 1;

FIG. 3 is a block diagram illustrating a process for 20 detecting and classifying both anomalous and normal behavior among self-organized clusters in an output set produced by the clustering methods of FIG. 2 according to one or more selected metrics; and,

FIG. 4 is a schematic illustration of multiple independent 25 private networks coupled to an IDS service provider in accordance with the inventive arrangements.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is an IDS which has been configured to perform anomaly based event detection, and in 30 particular, intrusion detection, based upon a robust analysis of network traffic vectors derived from granular network packet fields stored in a database. Specifically, the granular network traffic vectors can include scalar values for individual fields in a network packet, such as a network packet 35 which conforms to TCP/IP, UDP/IP, ICMP/IP and the like. Notably, each field can be captured in real-time and stored in a different record in the database so that feature vectors can be constructed from selected combinations of the fields.

Once the feature vectors have been constructed, a multi-variate analysis can be performed upon the feature vectors. 40 For example, one or more self-organizing clustering methodologies can be applied to the feature vectors to produce a set of clusters. Subsequently, a correlative analysis can be performed upon the set of clusters based upon either manually 45 or heuristically chosen metrics, for example the Euclidean or non-Euclidean spherical distance between individual clusters in the set. A deviation between the selected metrics and the individual clusters can indicate anomalous behavior. As a result, the anomalous behavior can be classified as either an event of significance, or a permissible deviation.

Where the anomalous behavior has been classified as an 50 event, the feature vectors which gave rise to the individual clusters associated with the anomalous behavior can be further examined to determine whether an unauthorized network intrusion has occurred. Alternatively, the feature vectors which gave rise to the individual clusters associated 55 with the anomalous behavior can be further examined to determine whether a network condition has arisen, such as the execution of an errant application or a failure in a network device which inhibits the performance of the network or a denial-of-service attack. Importantly, the classification of the anomalous behavior can be provided as feedback to the detection of subsequent anomalous behavior. Thus, over time the detection and classification of anomalous behavior can improve in accuracy as the self-organizing nature of the system adapts to the changing network environment.

## US 7,260,846 B2

7

FIG. 1 is a schematic illustration of a private network which has been configured with an IDS in accordance with the inventive arrangements. The private network **150** can include, for example, one or more servers **170** and coupled workstations **160**. Authorized client computing devices **110** can access the private network **150** over the computer communications network **130** along a communications path **195** in a conventional manner. In that regard, one or more security appliances **140**, such as a firewall, can limit access to the private network **150** in accordance with pre-configured firewall tables (not shown).

The private network **150** shown in FIG. 1 can be subjected to the malicious hacking activities of one or more unauthorized intruders **120** which can attempt to penetrate the restrictions imposed by security appliances **140**. To combat the malicious hacking activities, an IDS **200** can be coupled to the communications path **195** between the unauthorized intruder **120** and the target device in the private network **150**. Specifically, the IDS **200** can be disposed about the communications path **195** via a portion of the computer communications network **130**. In this way, the IDS **200** can monitor network traffic flowing from the unauthorized intruder **120** in order to detect an attack.

To detect an attack, the IDS **200** can monitor and analyze the contents of a database **100** such as a relational database or an object database. The contents can include granular elements of network packets which can be extracted from the network traffic flowing across the communications path **195**. More particularly, a packet sniffer **180** can extract network packets from the network traffic either in an exclusive or in an inclusive manner. For instance, the packet sniffer **180** can extract all network packets from the network traffic flowing along the communications path **195**. Alternatively, the packet sniffer **180** can extract network packets from the network traffic selectively according to one or more pre-configured selection filters. In any case, a logger **190** can parse the extracted packets along protocol boundaries into the constituent components forming each extracted network packet and can store the constituent components in the database **100**.

Importantly, it is to be understood by one skilled in the art that the network topology illustrated in FIG. 1 merely represents an exemplary network topology with which the IDS **200** of the present invention can be explained contextually. In consequence, the skilled artisan will recognize that the IDS **200** of the invention can be adapted for use with other network topologies such as the case where multiple private networks can be monitored by the IDS **200**. In the case of multiple private networks, it is to be further understood that each domain within each private network can include one or more server and workstation computing devices, in addition to any number of attached network addressable devices, such as printing devices, routing and switching appliances, security devices, and the like.

Significantly, it is a distinct advantage of the IDS **200** of the present invention that the sniffer **180** and logger **190**, in concert, can extract and store the constituent components of network packets stemming from network traffic for multiple private networks. In particular, by populating the database **100** with granular packet values from multiple private networks, the IDS **200** can undertake a correlative analysis not only in regard to traffic stemming from a single protected private network **150** such as that illustrated in FIG. 1, but also in regard to traffic stemming from multiple, independently operated private networks **150** as shown in FIG. 3. Accordingly, the IDS **200** can be deployed in the context of a managed service provider (MSP) model. In the MSP

8

model, however, wide-scale network anomalies, including multi-domain attacks, can be detected inasmuch as anomalous behavior can be detected across multiple networks which heretofore would not be possible in reference to conventional IDS technology.

FIG. 2 is a flow chart illustrating a process for performing intrusion detection using the IDS **200** of FIG. 1. Beginning in block **220**, a packet sniffer can extract network traffic **210** flowing across a communications path coupled to the IDS of the present invention. The network traffic **210** can be extracted exclusively or inclusively according to pre-configured filter rules applied to the packet sniffer. Packet sniffers are well-known in the art and include, for instance, the open-source Snort™ tool able to extract and log whole network packets as the network packets flow across a network interface device communicatively linked to the Snort™ software tool. Still, the invention is not limited in regard to the particular sniffer employed and other packet sniffing tools can suffice, for example Sniffer™ and Sniffer Basic™ manufactured by Network Associates, Inc. of Santa Clara, Calif., United States, Etherapeek™ manufactured by Wildpackets, Inc. of Walnut Creek, Calif., United States, and OptiView Integrated Network Analyzer Pro Gigabit™, manufactured by Fluke Networks of Everett, Wash., United States.

In any case, a sniffer either can be extended or wholly configured to parse extracted network packets into their constituent components. In that regard, a parser **230** can de-construct the network packets along known protocol field boundaries, such as destination and source IP address, time-to-live, payload size, packet type, type of service, etc. Subsequently, selected ones of the de-constructed fields can be stored in separate records in the database **240** and can be associated with the particular socket to which the packet belongs. Optionally, where the IDS has been deployed in an MSP environment, each field can be stored in a record in the database along with a reference to an associated customer and target device in the customer's private network.

In block **250**, a vector builder in a feature extraction process can select individual ones of the network packet fields to be included in the construction of a multi-dimensional vector. Additionally, global fields can be included in the construction of the multi-dimensional vectors, such as a customer identifier, or device identifier. Notably, the feature extraction process is not limited strictly to the construction of a multi-dimensional vector using the scalar values of selected fields. Rather, it can be helpful to include in the feature vector programmatically determined scalar values such as histogram data for particular scalar fields of the network packet such as frequency data for a specific field.

In any case, in block **250**, multi-dimensional vectors can be constructed using the chosen features produced in block **250**. Specifically, the vector builder can process the records in the database **240** to identify pertinent fields associated with a particular "conversation" or socket. As the vector builder locates the pertinent fields, a multi-dimensional vector for that socket can be constructed. Likewise, for other ones of the network data corresponding to other "conversations" or sockets, other multi-dimensional vectors can be constructed until a set of multi-dimensional vectors has been assembled for at least a selection of the granular network packet data associated with particular sockets represented in the database **240**.

In block **260**, a vector separation system can reduce the dimensionality of the multi-dimensional vectors in order to simplify a subsequent multi-variate analysis. In particular, components of the multi-dimensional vectors which appear

## US 7,260,846 B2

9

to be redundant, irrelevant, or otherwise insignificant relative to other interested components can be eliminated across all or a selection of the multi-dimensional vectors. For instance, a well-known principal component analysis can be applied to the multi-dimensional vectors in order to facilitate the reduction of the multi-dimensional vectors. In consequence, a set of reduced vectors can be produced.

In block 270, one or more self-organizing clustering methodologies can be applied concurrently or sequentially to the set of reduced vectors. Clustering methodologies are known in the art and include, for example, Kohonen self-organizing map (SOM) analysis, principal component analysis, multi-dimensional scaling analysis, principal curve analysis, wavelet analysis, and neural networks analysis, among others. Once, the reduced vectors have been processed by the multiple clustering methodologies in block 270, one or more metrics can be selected in block 280 for purposes of establishing a correlation between the output sets of the processed reduced multi-dimensional vectors. The chosen metric can be selected manually or in an heuristic fashion. In either case, in block 290 a classifier can identify from any established correlations whether an anomaly has been detected. For instance, the correlative output can be processed in a neural net or through a decision tree. In any case, the classification process of block 290 can identify either normal traffic or an attack.

FIG. 3 is a block diagram illustrating a process for detecting and classifying anomalous behavior among self-organized clusters in an output set produced by the clustering methods of FIG. 2 according to one or more selected metrics. As shown in FIG. 3, a set of reduced vectors 310 can be processed by one or more clustering methodologies 320. As is well-known in the art of multi-variate analysis, each self-organizing clustering methodology 320 can produce a self-organized mapping 340 of clusters 330. Based upon selected metrics 350, correlations can be evaluated to identify anomalous conditions through the application of an anomaly detection process 360. Though, any suitable metric can suffice, notable examples include a specified Euclidean distance between individual ones of the clusters 330, a specified surface area or volume of space between clusters 330, or a non-Euclidean specified spherical distance between clusters 330.

In any case, by detecting correlations which violate the selected metrics 350, the anomaly detection process 360 can produce a set of candidate clusters 370 which may or may not indicate a network fault or a network intrusion. Rather, the candidate cluster 370 merely indicate that an anomaly has been detected based upon a deviation in an ordinarily expected correlation between clusters 330 in the set as defined by one or more selected metrics 350. By comparison, the classifier 380 can assist in the identification of an actual network fault, a network intrusion or a change in network performance.

In that regard, the classifier 380 can programmatically identify a network fault, a change in network performance, or a network attack according to pre-specified rules, such as whether the deviation of the correlation between clusters 330 exceeds a threshold value. Alternatively, the classifier 380 can provide a manual mechanism for an operator to determine whether an attack or fault has occurred, or whether the anomalous behavior should be accepted at that time and going forward as normal behavior. In either case, the classifier 380, in addition to the anomaly detection process 360 can benefit from the classification of anomalous behavior exemplified among the candidate clusters 370 through the use of constructive feedback.

10

By reference both to FIGS. 3 and 4, one skilled in the art will recognize that by applying the correlative analysis to clusters derived from reduced vectors constructed from data destined for multiple domains among multiple private networks, attacks and network faults can be identified which would not be identifiable through the use of pattern matching techniques associated with conventional signature based systems. Moreover, as the database of the present invention includes packet data derived from multiple network sources, anomalous behavior can be detected across multiple domains which can permit the further identification of otherwise undetectable attacks and network faults. Finally, the use of a database to store multi-domain packet data permits rich querying of the database content so that the necessary correlations can be computed, even across multiple network domains.

The IDS of the present invention can be realized in hardware, software, or a combination of hardware and software. An implementation of an IDS and an intrusion detection method of the present invention can be realized in a centralized fashion in one computer system, or in a distributed fashion where different elements are spread across several interconnected computer systems. Any kind of computer system, or other apparatus adapted for carrying out the methods described herein, is suited to perform the functions described herein.

A typical combination of hardware and software could be a general purpose computer system with a computer program that, when being loaded and executed, controls the computer system such that it carries out the methods described herein. The present invention can also be embedded in a computer program product, which comprises all the features enabling the implementation of the methods described herein, and which, when loaded in a computer system is able to carry out these methods.

Computer program or application in the present context means any expression, in any language, code or notation, of a set of instructions intended to cause a system having an information processing capability to perform a particular function either directly or after either or both of the following a) conversion to another language, code or notation; b) reproduction in a different material form. Significantly, this invention can be embodied in other specific forms without departing from the spirit or essential attributes thereof, and accordingly, reference should be had to the following claims, rather than to the foregoing specification, as indicating the scope of the invention.

The invention claimed is:

1. An intrusion detection system (IDS) comprising:  
a traffic sniffer executing in a computing system for extracting network packets from passing network traffic;  
a traffic parser executing in a computing system configured to extract individual data from defined packet fields of said network packets;  
a traffic logger executing in a computing system configured to store individual packet fields of said network packets in a database;  
a vector builder executing in a computing system configured to generate multi-dimensional vectors from selected features of said stored packet fields;  
at least one self-organizing clustering module executing in a computing system configured to process said multi-dimensional vectors to produce a self-organized map of clusters;  
an anomaly detector executing in a computing system able to detect anomalous correlations between indi-

## US 7,260,846 B2

**11**

vidual ones of said clusters in said self-organized map based upon at least one configurable correlation metric; and

a classifier executing in a computing system configured to classify detected anomalous correlations as one of an alarm behavior.

2. IDS of claim 1, wherein said database is a relational database.

3. The IDS of claim 1, wherein said at least one self-organizing clustering module is configured to perform at least one of a Kohonen self-organizing map analysis, a principal component analysis, an multi-dimensional scaling analysis, a principal curve analysis, a wavelet analysis, and a neural network analysis.

4. The IDS of claim 1, wherein said at least one configurable correlation metric is selected from the group consisting of a heuristically determined metric and a manually specified metric.

5. The IDS of claim 1, wherein said at least one configurable correlation metric is a distance metric selected from the group consisting of a Euclidean distance metric and a non-Euclidean distance metric.

6. The IDS of claim 1, wherein said classifier is a weighted classifier configured to weight individual ones of said anomalous correlations according to a corresponding self-organizing clustering module used to produce particular clusters between which said individual ones of said anomalous correlations are detected.

7. An intrusion detection method comprising the steps of: monitoring network traffic passing across a network communications path;

extracting network packets from said passing traffic; storing individual components of said network packets in a database;

constructing multi-dimensional vectors from at least two of said stored individual components and applying at least one multi-variate analysis to said constructed multi-dimensional vectors, said at least one multi-variate analysis producing a corresponding output set;

establishing a correlation between individual output sets based upon a selected metric to identify anomalous behavior; and,

classifying said anomalous behavior as an event selected from the group consisting of a network fault, a change in network performance and a network attack.

8. The method of claim 7, wherein said storing step comprises the steps of:

identifying protocol boundaries in each extracted network packet; and,

storing data from each field separated by said identified protocol boundaries in a separate record in said database.

**12**

9. The method of claim 8, further comprising the step of storing with each said individual component in said separate record in said database, data associating said individual component with at least one of a corresponding target network device, a corresponding network socket, and a corresponding customer.

10. The method of claim 7, wherein said step of applying at least one multi-variate analysis to said constructed multi-dimensional vectors comprises the steps of:

reducing said constructed multi-dimensional vectors; and, applying at least one self-organizing clustering methodology to said reduced multi-dimensional vectors, said application of said at least one self-organizing clustering methodology producing a corresponding output set of clusters.

11. The method of claim 10, wherein said establishing step comprises the steps of:

loading at least one selectable metric; correlating individual ones of said clusters in said output set;

determining whether any of said correlations deviate from said loaded at least one selectable metric; and, for each one of said correlated clusters in said output set which deviates from said loaded at least one selectable metric, labeling said deviating correlated cluster as exhibiting anomalous behavior.

12. An intrusion detection method comprising the steps of:

monitoring network traffic passing across a network communications path destined for multiple target devices in multiple independent network domains and extracting network packets from said passing traffic;

identifying protocol boundaries in each extracted network packet and storing data from each field separated by said identified protocol boundaries in a database;

associating said data in said database with at least one of a corresponding target device, a target network domain, a target customer, and a target customer sub-net; processing said stored data using at least one self-organizing clustering method to establish correlations between fields of different network packets destined for different ones of said multiple independent network domains; and,

identifying a network attack, a network fault, or a change in network performance based upon said established correlations.

\* \* \* \* \*

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : 7,260,846 B2  
APPLICATION NO. : 11/367950  
DATED : August 21, 2007  
INVENTOR(S) : Christopher W. Day

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the title page of the Patent, item (73) Assignee, please update the location of the assignee to Ashburn instead of Herndon.

On the title page of the Patent, please insert item (60), entitled “Related U.S. Application Data” and under this section, please insert the following sentence: -- This patent is a Divisional of U.S. Application No. 10/208,485, filed July 30, 2002, now U.S. Patent No. 7,017,186, issued on March 21, 2006. --.

In the Specification

At Column 1, Line 2, underneath the title INSTRUCTION DETECTION SYSTEM, please insert the heading -- CROSS-REFERENCE TO RELATED APPLICATIONS -- and underneath the heading CROSS-REFERENCE TO RELATED APPLICATIONS, please insert the following sentence: -- This patent is a Divisional of U.S. Application No. 10/208,485, filed July 30, 2002, now U.S. Patent No. 7,017,186, issued on March 21, 2006. --.

Signed and Sealed this  
Twenty-fifth Day of February, 2014



Michelle K. Lee  
Deputy Director of the United States Patent and Trademark Office